

**HEARING ON REMOVING SOCIAL SECURITY
NUMBERS FROM MEDICARE CARDS**

JOINT HEARING
BEFORE THE
SUBCOMMITTEE ON SOCIAL SECURITY
AND
SUBCOMMITTEE ON HEALTH
OF THE
COMMITTEE ON WAYS AND MEANS
U.S. HOUSE OF REPRESENTATIVES
ONE HUNDRED TWELFTH CONGRESS
SECOND SESSION

—————
AUGUST 1, 2012
—————

SERIAL 112-SS19/HL14

—————

Printed for the use of the Committee on Ways and Means



U.S. GOVERNMENT PRINTING OFFICE

80-316

WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON WAYS AND MEANS

DAVE CAMP, Michigan, *Chairman*

WALLY HERGER, California	SANDER M. LEVIN, Michigan
SAM JOHNSON, Texas	CHARLES B. RANGEL, New York
KEVIN BRADY, Texas	FORTNEY PETE STARK, California
PAUL RYAN, Wisconsin	JIM MCDERMOTT, Washington
DEVIN NUNES, California	JOHN LEWIS, Georgia
PATRICK J. TIBERI, Ohio	RICHARD E. NEAL, Massachusetts
DAVID G. REICHERT, Washington	XAVIER BECERRA, California
CHARLES W. BOUSTANY, JR., Louisiana	LLOYD DOGGETT, Texas
PETER J. ROSKAM, Illinois	MIKE THOMPSON, California
JIM GERLACH, Pennsylvania	JOHN B. LARSON, Connecticut
TOM PRICE, Georgia	EARL BLUMENAUER, Oregon
VERN BUCHANAN, Florida	RON KIND, Wisconsin
ADRIAN SMITH, Nebraska	BILL PASCRELL, JR., New Jersey
AARON SCHOCK, Illinois	SHELLEY BERKLEY, Nevada
LYNN JENKINS, Kansas	JOSEPH CROWLEY, New York
ERIK PAULSEN, Minnesota	
KENNY MARCHANT, Texas	
RICK BERG, North Dakota	
DIANE BLACK, Tennessee	
TOM REED, New York	

JENNIFER SAFAVIAN, *Staff Director and General Counsel*

JANICE MAYS, *Minority Chief Counsel*

SUBCOMMITTEE ON SOCIAL SECURITY

SAM JOHNSON, Texas, *Chairman*

KEVIN BRADY, Texas	XAVIER BECERRA, California
PATRICK J. TIBERI, Ohio	LLOYD DOGGETT, Texas
AARON SCHOCK, Illinois	SHELLEY BERKLEY, Nevada
RICK BERG, North Dakota	FORTNEY PETE STARK, California
ADRIAN SMITH, Nebraska	
KENNY MARCHANT, Texas	

SUBCOMMITTEE ON HEALTH

WALLY HERGER, California, *Chairman*

SAM JOHNSON, Texas	FORTNEY PETE STARK, California
PAUL RYAN, Wisconsin	MIKE THOMPSON, California
DEVIN NUNES, California	RON KIND, Wisconsin
DAVID G. REICHERT, Washington	EARL BLUMENAUER, Oregon
PETER J. ROSKAM, Illinois	BILL PASCRELL, JR., New Jersey
JIM GERLACH, Pennsylvania	
TOM PRICE, Georgia	
VERN BUCHANAN, Florida	

CONTENTS

	Page
Advisory of August 1, 2012 announcing the hearing	2
WITNESSES	
Tony Trenkle, Chief Information Officer and Director, Office of Information Services, Centers for Medicare and Medicaid Services, Department of Health and Human Services, Baltimore, MD	8
Kathleen King, Director, Health Care, accompanied by Daniel Bertoni, Director, Education, Workforce, and Income Security, Government Accountability Office	21

**HEARING ON REMOVING SOCIAL SECURITY
NUMBERS FROM MEDICARE CARDS**

WEDNESDAY, AUGUST 1, 2012

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:36 a.m., in Room 1100, Longworth House Office Building, the Honorable Sam Johnson [chairman of the subcommittee] presiding.
[The advisory of the hearing follows:]

HEARING ADVISORY

Chairmen Johnson and Herger Announce a Hearing on Removing Social Security Numbers from Medicare Cards

Wednesday, August 1, 2012

House Ways and Means Social Security Subcommittee Chairman Sam Johnson (R-TX) and Health Subcommittee Chairman Wally Herger (R-CA) today announced that the Subcommittees will hold a joint hearing on removing Social Security numbers from beneficiaries' Medicare cards. **The hearing will take place on Wednesday, August 1, 2012, in 1100 Longworth House Office Building, beginning at 9:30 A.M.**

In view of the limited time available to hear from witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing. A list of invited witnesses will follow.

BACKGROUND:

In 2010, according to the U.S. Department of Justice, seven percent of households in the U.S., or about 8.6 million households, had a least one member age 12 or older who experienced identity theft. Of these households, over 1 million were headed by seniors, age 65 and older. The Social Security number (SSN) is especially valuable to identity thieves as it serves as the key to authenticating an individual's identity in order to open accounts or obtain other benefits in the victim's name.

The Government Accountability Office (GAO) first recommended removing the SSN from government documents in 2002. In 2007, President George W. Bush's Identity Theft Task Force found that the SSN is "the most valuable commodity for an identity thief" and its first recommendation was to reduce the unnecessary use of SSNs. That same year, the White House Office of Management and Budget issued a directive to all federal agencies to develop a plan for reducing the use of SSNs in government transactions and to explore alternatives to their use. In 2008, the Social Security Administration (SSA) Inspector General found that displaying SSNs on beneficiary Medicare cards unnecessarily places millions of Americans at risk for identity theft and recommended that the SSN be removed from Medicare cards. Also in 2008, the House of Representatives passed H.R. 6600, the "Medicare Identity Theft Prevention Act of 2008," introduced by Representatives Lloyd Doggett (D-TX) and Sam Johnson (R-TX), directing the Secretary of Health and Human Services (HHS) to establish cost-effective procedures to ensure that SSNs are not included on Medicare cards moving forward. This legislation passed the House by voice vote on September 28, 2008. Unfortunately, the Senate did not act on this legislation.

Today, nearly 50 million Medicare cards display SSNs, the main component of the health insurance claim number (HICN). The SSA and the Railroad Retirement Board assign HICNs to eligible Medicare beneficiaries. The HHS Centers for Medicare and Medicaid Services (CMS) administers the Medicare program and relies on the HICN for administering Medicare benefits, including requiring beneficiaries to present the HICN to document eligibility for Medicare services and requiring approximately 1.4 million providers to use the HICN for billing services.

To date, CMS has not developed a plan for removing the SSN from the Medicare card to protect beneficiaries from identity theft and protect taxpayers from fraudulent billing. In response to a July 2010 bipartisan request from the Committee on Ways and Means, CMS reported in November 2011 its estimates of three potential options for removing SSNs from Medicare cards, each projected to cost more than \$800 million, nearly triple the amount the agency had preliminarily estimated in 2006. CMS also estimated that the change would take four years to test and imple-

ment and cited the risks to its systems and those of its provider and health care partners if the necessary resources were not provided. On September 13, 2011, Chairman Sam Johnson and Congressman Lloyd Doggett asked GAO to examine the lessons learned from the efforts of the Department of Defense and Veterans Affairs to remove SSNs from their identification cards and later asked GAO to review CMS's 2011 report, including the options and their estimated costs.

In announcing the hearing, Chairman Johnson said, **“Seniors are urged not to carry their Social Security card to protect their Social Security number, but at the same time are being told they must have their Medicare card with them at all times in order to get health care. This makes no sense. Many agencies in the public and private sector have removed the Social Security number from their benefit or ID cards to protect people, yet CMS refuses to protect the 48 million Medicare beneficiaries from ID theft by doing the same. That’s why Congressman Lloyd Doggett and I have introduced H.R. 1509, removing the Social Security number from the Medicare card and reducing the ID theft danger that CMS has long ignored.”**

In announcing the hearing, Chairman Herger said, **“It is puzzling why CMS has not taken commonsense steps to protect Medicare beneficiaries from preventable identity theft by removing Social Security numbers from their Medicare cards. Other federal health programs and private health insurance plans invested in these changes years ago. This hearing enables the Subcommittees to explore whether CMS has a plan to remove Social Security numbers from beneficiary cards and determine whether its previous analysis in this area is reliable.”**

FOCUS OF THE HEARING:

The Subcommittees will examine options for removing SSNs from Medicare cards, including the cost and impact of doing so, along with why CMS has failed to develop and execute a plan to remove the SSN from beneficiary Medicare cards.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Any person(s) and/or organization(s) wishing to submit for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, <http://waysandmeans.house.gov>, select “Hearings.” Select the hearing for which you would like to submit, and click on the link entitled, “Click here to provide a submission for the record.” Once you have followed the online instructions, submit all requested information. ATTACH your submission as a Word document, in compliance with the formatting requirements listed below, **by the close of business on Wednesday, August 15, 2012**. Finally, please note that due to the change in House mail policy, the U.S. Capitol Police will refuse sealed-package deliveries to all House Office Buildings. For questions, or if you encounter technical problems, please call (202) 225-1721 or (202) 225-3625.

FORMATTING REQUIREMENTS:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission, but we reserve the right to format it according to our guidelines. Any submission provided to the Committee by a witness, any supplementary materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission or supplementary item not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. All submissions and supplementary materials must be provided in Word format and **MUST NOT** exceed a total of 10 pages, including attachments. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record.

2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material

not meeting these specifications will be maintained in the Committee files for review and use by the Committee.

3. All submissions must include a list of all clients, persons and/or organizations on whose behalf the witness appears. A supplemental sheet must accompany each submission listing the name, company, address, telephone, and fax numbers of each witness.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202-225-1721 or 202-226-3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Note: All Committee advisories and news releases are available on the World Wide Web at <http://www.waysandmeans.house.gov/>.

Chairman JOHNSON. Good morning. We welcome our colleagues from the Subcommittee on Health, who join the Social Security Subcommittee, today to focus on the importance of removing Social Security numbers from the Medicare cards.

For many years now, protecting the Social Security number has been a priority of the Ways and Means Committee that both sides agree on. So far this session, we have had numerous hearings on the role of Social Security numbers and the growing crime of identity theft. We have learned how identity thieves prey on anyone, including those most vulnerable, like seniors and children, even children who have died.

According to the Government Accountability Office, Social Security numbers are the identifier of choice, and are used for all sorts of financial transactions. In an April 2007 report, President Bush's Identity Theft Task Force identified the Social Security number as the most valuable commodity for an identity thief. It is no wonder the Department of Justice reports that 7 percent, or 8.6 million households had someone over the age 12 experience identity theft.

We all know Americans are told not to carry their Social Security cards to protect their identity in case a wallet is lost or stolen. Yet seniors are told they must carry their Medicare card, which displays a Social Security number. Not only does this make no sense, it puts Medicare beneficiaries at risk.

In 2007, the White House Office of Management and Budget issued a directive to all federal agencies to develop plans for reducing the use of Social Security numbers—2007; remember that date.

The Department of Defense and Veterans Affairs are now phasing out the use of Social Security numbers on their ID and Medicare cards. I applaud them for taking this action and for taking this action on their own. And some of our largest federal agencies, along with the most private insurance providers, can stop public display of Social Security numbers. The Centers for Medicare and Medicaid, or CMS, should too.

If CMS won't do what is right for America's Medicare beneficiaries, then Congress must act. That is why, along with my fellow Texan and Subcommittee on Social Security member, Congressman Lloyd Doggett, I have introduced legislation H.R. 1509, the Medicare Identity Theft Prevention Act of 2011. Our bill directs the Secretary of Health and Human Services to remove Social Se-

curity numbers from Medicare cards. A similar bill of ours passed the House with overwhelming bipartisan support in 2008 on a voice vote.

I thank my colleague from Texas for his work on this important issue, and all my committee colleagues for their support. I hope we will soon get this important legislation behind us. I thank each of our witnesses for sharing their findings and recommendations, and look forward to hearing your testimony.

I now recognize the Ranking Member, Mr. Becerra, for his opening statement.

Mr. BECERRA. Mr. Chairman, thank you very much. Identity theft is a serious problem, and seniors and disabled Americans are particularly vulnerable. Nearly nine million Americans a year have their identities stolen. According to the Federal Trade Commission, a typical theft costs a victim somewhere around \$500. That is a significant loss to someone who might be living on a fixed income. In a worst case scenario, thieves often will steal an average of about \$13,000 from a victim. And those victim spend about an average of 130 hours trying to clear their credit and prevent additional theft.

Seniors and disabled Americans are particularly vulnerable here. First, of course, we know that they have low incomes, so even a modest theft can be devastating. The median income of seniors in America, a senior household, would be somewhere around \$25,000 a year. And more than half of disabled Americans receiving Social Security and Medicare live in poverty, even with their Social Security benefits included.

And, of course, secondly, we know that seniors and disabled Americans often carry their Social Security numbers on their person. That makes them, of course, more available to thieves. I support removing the Social Security number from the Medicare card, which too many of our seniors carry on their person.

But making seniors more secure will require resources. Although it may sound simple, giving 49 million Americans new Medicare ID numbers and making sure that they can still fully access their benefits is a big job. The job is made more difficult because a series of Republican budget cuts has left the Centers for Medicare and Medicaid Services and the Social Security Administration struggling to keep up with their basic work just as the Baby Boomers, of course, are reaching their retirement age.

Since 2010, the Social Security field offices which take Medicare applications, issue Medicare cards, and provide in-person customer service to Medicare beneficiaries have lost nearly 2,300 employees, about 8 percent of their total staff, to budget cuts. Social Security offices are closing to the public half an hour early. And waiting times for phone service and initial disability benefits are rising.

Here in the House, the Republican Majority recently proposed cutting Social Security's fiscal year 2013 budget by nearly \$800 million below the 2012 levels. Short-changing Social Security makes it likely that the agency will have to furlough or lay off staff, and may create a backlog of retirement applications for the first time in our history.

Similarly, CMS funding has failed to keep up with their growing responsibilities. Their per-beneficiary operating budget has de-

clined by 14 percent since 2004. Once again, any cuts in any House budget to CMS's funding could lead to more devastating impact for those Medicare beneficiaries. And funding we see may actually reduce by about \$400 million in the House Republican budget.

We need to provide the resources so that CMS can better protect seniors from identity theft. The Bush Administration, back in 2004, failed to solve this problem when GAO first identified it. And it is still not solved, despite strong support in our committee and the House, passing Chairman Johnson and Mr. Doggett's bill, H.R. 6600 back in 2008.

Congress first directed HHS to address this issue in 2005 in the Labor, Health and Human Services, and Education appropriations bill. In 2007, the Bush Administration failed to make CMS comply with an executive order to eliminate unnecessary use of the Social Security number. And, most recently, CMS produced a cost estimate for removing the Social Security number from Medicare cards, as we requested. But as GAO has pointed out, there may be significant flaws in that estimate.

I hope that CMS is ready to partner with us to solve this problem, starting with providing a comprehensive and reliable cost estimate.

Mr. Chairman, this is an issue that we have been working on for some time. I hope that we are able to work together with the Administration to get this done, because millions of Americans depend on getting their Social Security and Medicare benefits, and none of them should be facing the possibility of theft, simply so that people can steal their Social Security number and take advantage of them.

And so, with that, I am pleased to have our witnesses here, and I look forward to the hearing. And with that, I yield back the balance of my time.

Chairman JOHNSON. Thank you, Mr. Becerra. I now recognize the chairman of the Subcommittee on Health, Mr. Herger, for his opening statement.

Mr. HERGER. Thank you. I am pleased the subcommittees are meeting today to discuss what I consider to be a commonsense, bipartisan idea that will help protect our nation's seniors, brought before the committee by Chairman Johnson and Congressman Doggett.

Medicare beneficiaries from across the United States are affected by fraud and identity theft, including those in California, where nearly 100,000 beneficiaries have had their Social Security numbers compromised, according to CMS data. I am sure I am not the only member of this committee who has received letters for congressional action to remove Social Security numbers from Medicare cards.

A constituent of mine wrote about an interaction with CMS where he was told, after asking about removing Social Security numbers from Medicare cards, "We have always done it that way, and we don't intend to change it." He went on to state, "With identity theft running rampant in this country, it seems ridiculous that Medicare would refuse to stop this practice." I couldn't agree more.

While challenges lie ahead for the agencies involved in the process of removing Social Security numbers from public documents, I am very disappointed with the lack of leadership and interest in

this issue at the Centers for Medicare and Medicaid Services. To date, CMS has offered little beyond excuses and questionable reports. Interestingly, CMS did not appear too concerned about the cost and efforts involved with removing Social Security numbers when it mandated that private Medicare plans do so years ago.

When the Office of Management and Budget, under the previous Administration, issued a 2007 directive to all federal agencies to develop a plan to remove Social Security numbers, the Department of Defense and Veterans Administration acted. As a result, they are well underway toward full implementation of their plans. Presumably, these departments had the same logistical challenges that CMS faces, but they did not offer excuses. They offered a plan. And not only did they have a plan, but they also found a way to do it with existing funding.

CMS doesn't even have a plan to move forward, despite being directed to do so five years ago, and now professes to need nearly \$1 billion in additional funding to do so. The validity of the latest CMS cost estimates has been questioned by GAO. The new estimate is nearly three times more expensive, despite taking half as long to implement than it was predicted just a few years ago. It is becoming clear to me that CMS simply isn't interested in taking this commonsense approach to protect seniors and people with disabilities from identity theft. Or, perhaps there is another reason.

As we all know, there is a key development that took place between the first estimate and the second estimate: the enactment and initial implementation of Obamacare. It has been widely reported that significant CMS resources, both financial and staffing, have been diverted from the Medicare program to implement non-Medicare Obamacare provisions such as exchanges and mandated health benefits. I can't help but wonder if this new cost estimate reflects just how thin Medicare has been stretched because of Obamacare, or perhaps that some in the Obama Administration recognize this as an opportunity to grab more money to implement Obamacare.

As you may know, the independent Congressional Budget Office has repeatedly stated that the Democrats' health care law drastically underfunded implementation efforts. If this is a simple money grab, perhaps that is why CMS has been unable to provide sufficient data or other information to support the cost estimates in its report. It is clear that a more complete and thorough cost analysis by CMS is necessary, one that is held to the standards we have come to expect in reports to Congress by federal entities. If CMS does not want to responsibly act, then Congress will require them to. Business as usual should not trump protecting Medicare beneficiaries.

Thank you, Chairman Johnson, and I yield back.

Chairman JOHNSON. The gentleman's time has expired. Thank you. I now recognize the Ranking Member on the Subcommittee on Health, Mr. Stark, who is also on the Ways and Means Social Security Subcommittee. Thank you.

Mr. STARK. Thank you, Mr. Chairman. And thank you for your work in this area, and you and my colleague, Congressman Doggett, for addressing a serious problem. Happily, I don't have this problem.

A lot of the question is what kind of an identity you have. Mine was stolen a while back, and that guy that stole it called me shortly thereafter and asked if I would please take the identity back, and—he was having trouble with it.

[Laughter.]

Mr. STARK. So, one way to do away with this problem is to sort out what kind of an identity you wish to have stolen. But we haven't done ourselves any good by coming up with a wide variety of estimates. As you indicated, three—or Mr. Herger indicated, between \$300 million and \$800 million. And GAO has criticized some of these analyses. And it will cost money. It will take a bit of bureaucratic effort to come up with a problem that doesn't sound—a solution to the problem. And I hope that we can proceed. It is a danger. And as the Internet and these world of social connections become broader, this problem will spread. And it is—I think we should encourage and support, with adequate funding, a means for our government agencies to tackle this problem as promptly as they can.

Thank you for the hearing, and thank Mr. Doggett for his work in this area.

Chairman JOHNSON. Thank you, Mr. Stark. As is customary—any Member is welcome to submit a statement for the hearing record.

Before we move on to our testimony today, I want to remind our witnesses to please limit your oral statements to five minutes, please. However, without objection, all the written testimony will be made part of the hearing record.

We have one panel today. Seated at the table are Tony Trenkle, Chief Information Officer and Director, Office of Information Services, Centers for Medicare and Medicaid Services, Department of Health and Human Services in Baltimore, Maryland. You could have more titles, could you?

Next is Kathleen King, Director, Health Care, accompanied by Daniel Bertoni, Director, Education, Workforce, and Income Security, Government Accountability Office.

Welcome, Mr. Trenkle. You may proceed.

STATEMENT OF TONY TRENKLE, CHIEF INFORMATION OFFICER AND DIRECTOR, OFFICE OF INFORMATION SERVICES, CENTERS FOR MEDICARE AND MEDICAID SERVICES, DEPARTMENT OF HEALTH AND HUMAN SERVICES, BALTIMORE, MARYLAND

Mr. TRENKLE. Thank you. Chairman Herger, Chairman Johnson and Herger, Ranking Members Becerra and Stark, and distinguished Members of the Subcommittees, I am pleased to be here today on behalf of the Centers for Medicare and Medicaid Services to discuss the use of the Social Security numbers on the Medicare identification cards.

CMS supports protecting beneficiaries from fraud and abuse and identity theft, and we understand the concerns that the use of the SSN causes for some beneficiaries. As a personal note, a couple weeks ago my aunt passed away suddenly. And as the executive of the estate, I had to go through the house and clear it out. And part of that was looking at her wallet. And in the wallet was both her

Social Security card and her Medicare card. So I understand, from a personal basis, what the risks are of carrying that in a public location by a person who is 89 years old.

CMS is happy to work with Congress to develop an approach for removing SSNs from the Medicare cards. And, depending on the time frame, reprioritizing work that Congress has given us. To that end, CMS has provided Congress with a cost estimate for removing SSNs from Medicare cards in 2006 and 2011. And I know some concerns have been expressed about the difference in cost between the 2006 and 2011 estimates. However, the 2011 estimate was updated to reflect additional options, a new time for implementation, a much more comprehensive review of impacted CMS systems, and an estimate for Medicaid costs, which was not in the 2006 report.

This update provided a rough order of magnitude of the cost to remove the SSN from the Medicare card, and clearly demonstrates that any change in the current system for beneficiary identification requires substantial investment of time, resources, and staff. We appreciate the analysis that our colleagues from the GAO conducted on our report and cost estimates. And we concur with the recommendation that we re-estimate the cost of removing the SSNs from Medicare cards, using a more rigorous and detailed approach. We have already begun work on that effort. We have identified staff to work on it, and also will be shortly awarding a contract to support that work.

It is important to remember—there was a question raised about the difference between us and DoD and VA—it is important to remember that we are much more intricately linked with SSA and the SSN. I worked in both agencies, and I know how tightly linked the two agencies are because it is a basis for identity—beneficiary authentic identification, fundamental to multiple systems, required to process and track beneficiary claims and enrollment, to conduct our anti-fraud and quality improvement offices and coordinate with SSA, Railroad Retirement Board, and state Medicaid.

As a health care organization, we annually process 1.3 billion Medicare claims from about a million providers on behalf of 50 million Medicare beneficiaries. Any change to Medicare card would impact each Medicare beneficiary, along with providers, health insurers, states, operations and systems of the primary agencies involved in the administration of Medicare.

CMS is determined that changes to Medicare card would involve 50 CMS systems and require sufficient planning and resources to ensure that beneficiaries and providers would not experience major disruptions. We believe, of the three options presented, the option to replace with a new identifier best meets the goals of reducing the risk of identity theft and preventing fraud, while minimizing the burden on beneficiaries and providers.

We share the concerns of the committee and others about potential identity theft and schemes that target Medicare beneficiaries. Given the budget and logistical challenges of removing the SSNs from Medicare cards, we have already taken a number of steps to protect beneficiaries from identity theft. We have removed the SSNs from the Medicare summary notices that are mailed to beneficiaries on a quarterly basis. And we have prohibited private Medi-

care, health, and prescription drug plans from using SSNs on enrollees' insurance cards.

We are engaged in education effort to provide beneficiaries with information on how to prevent medical identity theft and Medicare fraud, which includes educating them about steps to prevent identity theft and fraud, including posting information on the CMS website, and adding information to the Medicare handbook. We encourage our beneficiaries to review their billing statements and other medical reports to spot unusual or questionable charges.

So, in closing, I appreciate the concerns expressed by Congress and beneficiaries regarding the continued use of SSNs on Medicare cards. And I can assure you that CMS will work to protect beneficiaries from fraud, abuse, and identity theft, wherever possible. The Administration is happy to work with Congress to develop an approach to remove SSNs from the Medicare card. We pledge to continue our efforts to safeguard beneficiary identification numbers, maintain dialogue about options that Congress may wish to consider, ensure there is no disruption in beneficiary access to their Medicare services.

Though the costs and challenges of the Medicare cards that CMS has identified are real, these challenges can be mitigated with thoughtful planning. I appreciate the committee's ongoing interest in this issue, and can assure you that CMS is committed to working with Congress to identify ways to best protect beneficiaries' privacy. Thank you.

[The prepared statement of Tony Trenkle follows:]

11

STATEMENT OF

TONY TRENKLE

DIRECTOR OF THE OFFICE OF INFORMATION SERVICES AND CHIEF
INFORMATION OFFICER

CENTERS FOR MEDICARE & MEDICAID SERVICES

ON

REMOVING SOCIAL SECURITY NUMBERS FROM MEDICARE CARDS

BEFORE THE

U.S. HOUSE COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON SOCIAL SECURITY
AND SUBCOMMITTEE ON HEALTH

AUGUST 1, 2012

Hearing on Removing Social Security Numbers from Medicare Cards

August 1, 2012

Chairmen Johnson and Herger, Ranking Members Becerra and Stark, and distinguished members of the Subcommittees, I am pleased to be here today on behalf of the Centers for Medicare & Medicaid Services (CMS) to discuss the use of Social Security Numbers (SSNs) within Medicare.

CMS takes seriously the risk of identity theft for Medicare beneficiaries. We have removed SSNs from Medicare Summary Notices mailed to beneficiaries on a quarterly basis, and we have prohibited private Medicare health and prescription drug plans from using SSNs on enrollees' insurance cards (e.g., insurance cards for Medicare Advantage, cost contract, and Part D prescription drug plan enrollees). We are engaged in an education effort that provides beneficiaries with information on how to prevent medical identity theft and Medicare fraud. However, the SSN is used as the basis for beneficiary identification because it is fundamental to multiple CMS systems required to process and track beneficiary claims and enrollment, to conduct our antifraud and quality improvement efforts and to coordinate with the Railroad Retirement Board (RRB) and State Medicaid programs across the country.

In response to a request from the House Ways and Means Committee, CMS issued a report in November 2011 entitled *Update on the Assessment of the Removal of Social Security Numbers from Medicare Cards* (November 2011 Update), which examined three different options for removing SSNs from the Medicare card.¹ This report was an update to a 2006 report, *Removal of Social Security Number from the Medicare Health Insurance Card and Other Medicare Correspondence*.² As the November 2011 Update described, transitioning to a new identifier would be a task of enormous complexity and cost and one that, undertaken without sufficient planning, would present great risks to continued access to healthcare for Medicare beneficiaries.

¹ Centers for Medicare & Medicaid Services, Report to Congress: Update on the Assessment of the Removal of Social Security Numbers from Medicare Cards. November 2011.

² Centers for Medicare & Medicaid Services, Report to Congress: Removal of Social Security Number from the Medicare Health Insurance Card and Other Medicare Correspondence. October 2006.

Social Security Number as Medicare Health Insurance Claim Number (HICN)

From the creation of the Medicare program under the Social Security Act in 1965 until 1977, the Medicare program was administered by the Social Security Administration. While CMS is now responsible for the management of Medicare, the Social Security Administration and Medicare continue to rely on interrelated systems to coordinate both Social Security and Medicare eligibility. Medicare cards include a Health Insurance Claim Number (HICN) which is used as the beneficiary identification number for Medicare. Generally, the HICN is based upon a beneficiary's SSN, or in cases where a beneficiary's Medicare eligibility is based on the employment status and Medicare payroll tax contributions of another person, his or her spouse or parent's SSN. After determining Medicare eligibility, the Social Security Administration transmits the SSN and beneficiary identification code (BIC)³ to CMS for entry into the CMS Enrollment Database, the data repository for individuals who are or have ever been enrolled in Medicare. CMS then issues the Medicare card with the HICN to the beneficiary. The HICN serves as the primary identifier used for communication between the beneficiary and CMS, and is also used by providers who bill CMS, and for enrollment transactions with Medicare Advantage and prescription drug plans. CMS utilizes the HICN as a beneficiary's identifier in 50 internal CMS systems and in CMS communication with the Social Security Administration, State Medicaid programs, and other nonpayment partners.⁴

When receiving care, the beneficiary shows the provider or supplier their Medicare card with the HICN. The provider or supplier then uses the Medicare card information to check eligibility and to bill Medicare, a process that involves multiple CMS systems. Some examples of the CMS administrative systems that utilize the HICN are: enrollment, quality control, program integrity data for research purposes, and the coordination of benefits. Additionally, the eleven companies contracting with CMS for claims processing communicate with providers or suppliers using the HICN for remittance and payment.

³ The beneficiary identification code (BIC) is a letter code that appears after the SSN, which corresponds to the relationship of the cardholder to the individual whose work history enables the beneficiary to receive benefits.

⁴ Non-payment partners include: States, Railroad Retirement Board, Social Security Administration, Department of Defense/TriCare, Office of Personnel Management, Department of Veterans Affairs, Indian Health Service, End Stage Renal Disease Networks (REMIS), Department of Treasury (debt referrals), Quality Improvement Organizations and other quality contractors, Program Integrity Contractors, Employers, Federal and State Health Insurance Exchanges (future capability, as permitted by the HIPAA Privacy Rule.)

CMS Reports on the Removal of SSNs from Medicare Cards

CMS appreciates concerns about the ongoing use of SSNs on Medicare cards that have been expressed by beneficiaries and other stakeholders, including Members of Congress. CMS provided an initial examination of the potential challenges and costs posed by the removal of SSNs from Medicare cards in the 2006 report to Congress. In this report, CMS concluded that removing SSNs from Medicare cards would require extensive planning and would be a costly undertaking.

CMS' November 2011 Update provided a current analysis and cost estimate of options for removing SSNs from Medicare cards, as well as three distinct options for removal of SSNs from Medicare cards. Each of the three options evaluated in the November 2011 Update included cost estimates, estimated implementation timeframes, and potential impacts to beneficiaries, providers, insurers, States and other Federal agencies. It identified scenarios related to removal of the SSN from the Medicare card for all current and future Medicare beneficiaries.

CMS found that removing the SSN from Medicare beneficiary identification cards would have immediate and far reaching consequences. As a health care organization, Medicare annually processes about 1.3 billion claims from about 1.5 million providers on behalf of 52 million Medicare beneficiaries. Any change to the Medicare card would impact each Medicare beneficiary, along with health care providers, health insurers and States, as well as the operations and systems of the primary Federal agencies involved in the administration of Medicare—CMS, the SSA, and the Railroad Retirement Board (RRB).

Three Potential Implementation Scenarios Identified

The three scenarios identified in the November 2011 Update each present unique characteristics built around business processes that correlate to different benefits, potential risks and costs. All three implementation scenarios address the concern that the presence of the SSN on the Medicare card presents a risk for identity theft if the card is lost or stolen. As described below, only Scenario 1 replaces the HICN with an entirely new Medicare Beneficiary Identifier (MBI) for purposes of provider billing. As a result, only Scenario 1—the most costly and operationally

challenging of the three options— would allow the MBI used for billing Medicare to be terminated and replaced in the event it was used for fraudulent billing of Medicare.

Scenario One – Medicare Card and Number Replacement/New “MBI”

Under this scenario beneficiaries would receive a new Medicare card with a newly issued MBI, which they would use to receive services from providers. Providers would verify the new MBI and use it for CMS interactions. However, CMS internal systems would process claims and other transactions using the old HICN provided through the use of a translation utility. CMS interfaces with non-payment exchange partners would remain HICN-based, while interfaces with payment partners⁵ would use the new MBI. If a beneficiary presented her MBI card to a Government agency such as a SSA Field Office, that agency would convert the MBI to the HICN via a CMS query.

Under this scenario, if an MBI became compromised in some way— for example the number was used for some type of fraudulent purpose—CMS would have the ability to cancel the MBI, issue a new number and card to the Medicare beneficiary, and update its internal utility to use the new data for the MBI to HICN translation.

This scenario would help improve CMS’ ability to combat fraud, waste, and abuse since this would provide the ability to turn off an HICN similar to the way credit card companies are able to easily cancel a compromised credit card to stop fraudulent activity and then reissue a new number. Although CMS anticipates there are potential savings associated with an improved ability to turn off or eliminate compromised beneficiary identifiers, CMS cannot determine, at this time, to what extent a new non-SSN beneficiary identifier would more effectively address the problem of compromised identifiers compared to other approaches which identify and combat Medicare fraud currently under development.

Scenario Two - Medicare Card and Number Replacement/New “MBI” for Query Purposes Only

⁵ Payment exchange partners: Carriers/MACs/FIs/DME MACs, Providers, DME Suppliers, Part C Plans, Part D Plans

Under this scenario, beneficiaries would receive a new Medicare card with a newly issued MBI. Providers would use the new MBI to query CMS systems to obtain the corresponding old HICN. Unlike Scenario 1 where the providers would use the newly issued MBI to interact with CMS, providers would continue to use the current HICN (based on the SSN) to interact with CMS. CMS internal systems would conduct processing and interface with non-payment and payment exchange partners using the HICN. CMS would use the MBI to interact with beneficiaries. If a beneficiary presented her MBI card to a Government agency such as a SSA Field Office or health care provider, that agency or health care provider would convert the MBI to the HICN via a CMS query.

Scenario 2 would likely place a significant burden on the provider community. In Scenario 2, providers would need to develop the operating procedures and systems capability to: (1) collect a MBI from beneficiaries; (2) electronically request the HICN from Medicare; and (3) then use the HICN for billing purposes.

If the situation warranted, CMS would cancel an existing MBI, issue a new number and card, and update its internal utility to use the new data for the MBI to HICN translation. However, since the HICN remained the beneficiary identifier for billing purposes, CMS would have to use the same types of edits and controls it currently employs in the event a HICN becomes compromised. This scenario maintains the necessity of providers keeping the HICN on file for billing, which would still present a possible risk of identity theft in the event of a data breach in a provider's office.

Scenario Three – Partial HICN Display on Medicare Card

Under the third scenario presented in the November 2011 Update, beneficiaries would receive a new Medicare card with a modified HICN. The change to the Medicare card would be the obscuring of the first five digits of the beneficiary's SSN. This means the BIC portion of the HICN and the last four digits of the SSN would remain visible. Providers would manage verification and eligibility checks through one of the existing resources designed for that purpose. CMS internal systems would continue to conduct processing and interface with non-payment and payment exchange partners using the HICN. However, CMS internal systems,

payment and non-payment exchange partners would require system modifications to accommodate a change to the HICN input fields for verification and eligibility checks.

Since the HICN would remain the beneficiary identifier for billing purposes, CMS would have to use the same types of edits and controls it currently employs in the event a HICN were to become compromised. This scenario would require providers keep the HICN on file for billing, which would still present a possible risk of identity theft in the event of a data breach in a provider's office.

Costs for Implementation

As the Committee requested, the November 2011 Update provided cost estimates for scenarios for removing the SSN from Medicare cards along with the costs and timeframes associated with such options. The SSN-based HICN is the identifier used for 50 CMS systems, as well as for communication with the SSA, RRB, State Medicaid departments and private Medicare health and prescription drug plans. As a result of its widespread use as a foundational component in CMS and partner systems, all the options for changing the beneficiary identifier would be costly, and could require significant changes from the many stakeholders who need to accurately identify the more than 52 million beneficiaries who have Medicare cards with HICNs. In addition, there are substantial costs associated with outreach to those beneficiaries and their providers to ensure any transition goes smoothly, without disruptions in access to care. CMS would be committed to extensive outreach and education for beneficiaries, caregivers, and providers in order to ensure that any transition did not create a new opportunity for fraudsters to take advantage of beneficiary confusion associated with the transition to obtain beneficiaries' personal information.

The November 2011 Update estimated that it would require approximately \$812 million to \$845 million, depending on the implementation scenario. In general, Scenario 1 is expected to incur the highest costs, primarily based upon the expectation that providers would use the MBI in their interactions with CMS. This would require CMS to modify all systems that receive inquiries and billing transactions from providers to accept the MBI number and immediately interface with the translation utility to replace that with the HICN for internal processing.

Estimates for all three scenarios also considered the projected costs for SSA and RRB,⁶ as well as the changes necessary to State Medicaid systems. For beneficiaries dually eligible for Medicare and Medicaid, State Medicaid systems would need to recognize, accept, and transition to the use of a new beneficiary number, as well as incur the cost of matching historical data to the new identifier. In all three scenarios, the cost of converting CMS systems accounts for a significant portion of the cost. These costs include system development costs to cover the planning, gathering, development and implementation of new system changes and include Federal FTE and contractor labor, hardware and software updates for approximately 50 systems. Under all three scenarios, CMS, our Federal partners, and State Medicaid programs would expect to face substantial systems work at a significant cost.

Current CMS Efforts to Prevent Identity Theft

CMS shares the concerns of this Committee and others about the potential identity theft and schemes that target Medicare beneficiaries. Given the budgetary and logistical challenges of removing SSNs from Medicare cards, CMS has already taken a number of steps to protect beneficiaries from identity theft. We have also taken multiple actions to educate beneficiaries about steps they should take to prevent identity theft and fraud, including posting information on the CMS website⁷ and adding information to the annual “Medicare & You” Handbook.⁸

Increasing Beneficiary Awareness About Identify Theft

Outreach, education, and ongoing communication are consistently utilized to increase beneficiary awareness about minimizing opportunities for medical identity theft. CMS has a multi-pronged approach to educating beneficiaries and sensitizing them to this important issue that includes the CMS *Medicare & You* handbook and information available online at www.Medicare.gov⁹ and www.stopmedicarefraud.gov.¹⁰ Beneficiaries are provided with

⁶ SSA and RRB provided estimates of their respective projected costs for all three scenarios.

⁷ <http://www.medicare.gov/navigation/help-and-support/fraud-and-abuse/fraud-and-abuse-overview.aspx>

⁸ <http://www.medicare.gov/Publications/Pubs/pdf/10050.pdf>

⁹ Information includes “Protecting Medicare and You from Fraud,” which advises beneficiaries on how to protect themselves from identity theft.

¹⁰ Information includes “Medical Identity Theft & Medicare Fraud,” which offers advice on protecting personal information, what to look out for in fraud schemes, how to read Medicare bills, and how to report Medicare fraud or identity theft.

recommendations on who they should provide personal information to and what that information should be. In situations where they are suspicious or concerned about someone requesting personal information, assistance and support contact options are readily available. CMS also encourages our beneficiaries to review their Medicare billing statements and other medical reports in order to spot unusual or questionable charges. On March 7, 2012, Medicare announced the redesign of the quarterly Medicare Summary Notices (MSN) so that beneficiaries can more easily spot potential fraud or irregularities on claims submitted for their care.¹¹

CMS has also been partnering with the Administration for Community Living (ACL) to operate the Senior Medicare Patrol program - groups of senior citizen volunteers that educate and empower their peers to identify, prevent, and report identity theft and other forms of health care fraud. The SMP program empowers seniors through increased awareness and understanding of health care programs.

Since the SMP program's inception in 1997, the program has educated over 4.6 million beneficiaries in group or one-on-one counseling sessions and has reached an estimated 27 million people through SMP-led community education outreach events. Over 323,000 Medicare, Medicaid and other complaints of potential health care fraud have been resolved by SMPs or referred for further investigation.

Conclusion

CMS takes seriously our responsibilities to provide high quality health care to beneficiaries while also protecting the privacy of Medicare beneficiaries. CMS has implemented efforts to protect beneficiaries from identity theft through enhanced beneficiary communication, education on identifying and reporting fraud, waste, and abuse, and the importance of protecting Medicare ID numbers. CMS has also taken actions to minimize unnecessary use of SSNs by removing SSNs from Medicare Summary Notices and prohibiting Medicare private health and drug plans from using SSNs on enrollees' insurance cards.

¹¹<http://www.cms.gov/apps/media/press/release.asp?Counter=4298>

CMS appreciates the concerns expressed by Congress and beneficiaries regarding the continued use of SSNs on Medicare cards. However, we recognize that any effort to remove SSNs from Medicare cards would be an administratively complex and costly undertaking, and would require significant advance planning to ensure a smooth transition and appropriate education and outreach.

We pledge to continue our efforts to safeguard beneficiary identification numbers and to maintain dialogue about other options that Congress may wish to consider. I appreciate the Committee's ongoing interest in this issue, and can assure you that CMS is committed to working with Congress to identify ways to best protect beneficiaries' privacy.

Chairman JOHNSON. Welcome, Ms. KING. You are recognized.
Go ahead.

**STATEMENT OF KATHLEEN KING, DIRECTOR, HEALTH CARE;
ACCOMPANIED BY DANIEL BERTONI, DIRECTOR, EDUCATION,
WORKFORCE, AND INCOME SECURITY, GOVERNMENT ACCOUNTABILITY OFFICE**

Ms. KING. Chairman Johnson, Chairman Herger, ranking Members of the Subcommittees, and other Members of the Subcommittees, we are pleased to be here today to discuss our review of the options presented in the 2011 Report to Congress by CMS for removing Social Security numbers from Medicare cards, and the agency's cost estimates for these options.

More than 48 million Medicare cards display an SSN as part of the health insurance claim number, or HICN. The HICN plays an essential role in the administration of the Medicare program, and is used by CMS to interact with beneficiaries and providers, and by other agencies that play a role in determining an individual's eligibility for Medicare. For most people, the Social Security Administration is responsible for determining Medicare eligibility and assigning the HICN.

In response to a congressional request from some members of these subcommittees, CMS presented three options for removing the SSNs from Medicare cards. All three options would generally require similar efforts, including coordinating with stakeholders, converting information technology systems, conducting provider and beneficiary outreach, training of business partners, and issuing new cards.

Of the three options in CMS's report, we found that replacing the SSN with a new identifier for use by both beneficiaries and providers offers beneficiaries the greatest protection against identity theft, because the SSN would no longer be printed on the card. In addition, because providers would not need the SSN to interact with CMS, they would not be required to collect or maintain this information, reducing beneficiaries' vulnerability in the event of a provider data breach. This option may also prevent fewer burdens for providers, because they would not have to query a CMS database or call CMS to obtain beneficiaries' information.

CMS estimated that implementation would cost between \$803 million and \$845 million over 4 years, depending on the option selected. Approximately two-thirds of the total estimated cost are associated with modifications to state Medicaid IT systems and CMS's and its contractors' IT systems. We have four key concerns regarding the methods and assumptions CMS used to develop its cost estimates that raise questions about their reliability.

First, CMS did not use any standard cost estimating guidance in developing their estimates. Second, the procedures used to develop the estimates for the two largest cost categories, the Medicaid IT systems and the CMS IT systems, are questionable and not well documented. Third, we identified some inconsistencies in the assumptions used by CMS and SSA in developing the estimates. Finally, CMS did not take into account other factors, such as possible efficiencies that could be realized by combining IT modifications required to remove SSNs with related IT modernization efforts, or consider potential savings from not having to monitor compromised SSNs.

While CMS has identified options for removing the SSN from Medicare cards, the agency has not committed to a plan for this removal. Lack of progress on this key initiative leaves Medicare beneficiaries exposed to the possibility of identity theft.

In a report we are releasing today, we have recommended that CMS select an approach for removing the SSN from the Medicare card that best protects beneficiaries from identity theft and minimizes burdens for providers, beneficiaries, and CMS.

We have also recommended that CMS develop an accurate, well-documented cost estimate using standard cost estimating procedures.

Mr. Chairman, this concludes my prepared remarks. Happy to answer any questions.

[The prepared statement of Kathleen King follows:]

United States Government Accountability Office

GAO

Testimony
Before the Subcommittees on Social
Security and Health, Committee on Ways
and Means, House of Representatives

For Release on Delivery
Expected at 9:30 a.m. EDT
Wednesday, August 1, 2012

MEDICARE

Action Needed to Remove Social Security Numbers from Medicare Cards

Statement of Kathleen M. King
Director, Health Care

Daniel Bertoni
Director, Education, Workforce, and Income Security
Issues

To access this report
electronically, scan this
QR Code.
Don't have a QR code
reader? Several are
available for free online.



GAO-12-949T

Chairman Johnson, Chairman Herger, and Members of the Subcommittees:

We are pleased to be here today to discuss our review of the options presented by the Department of Health and Human Services (HHS) and its agency, the Centers for Medicare & Medicaid Services (CMS), for removing Social Security numbers (SSN) from Medicare¹ cards and the agency's cost estimates for these options.²

More than 48 million Medicare cards display an SSN as part of the health insurance claim number (HICN). The HICN plays an essential role in the administration of the Medicare program and is used by CMS to interact with beneficiaries and providers, and by other agencies that play a role in determining an individual's eligibility for Medicare.³ However, thieves can steal the information from Medicare cards to commit various acts of identity theft, such as opening fraudulent bank or credit card accounts or receiving medical services in a beneficiary's name. In 2010, 7 percent of households in the United States, or about 8.6 million households, had at least one member age 12 or older who experienced identity theft, according to U.S. Department of Justice figures. The estimated financial cost of identity theft during that year was approximately \$13.3 billion.⁴ Theft of this information can also result from a data breach—the unauthorized disclosure of a beneficiary's personally identifiable information.⁵ Between September 2009 and March 2012, the HHS Office for Civil Rights identified over 400 reports of provider data breaches

¹Medicare is the federal health insurance program for individuals over the age of 65, individuals under the age of 65 with certain disabilities, and individuals with end-stage renal disease.

²Centers for Medicare & Medicaid Services, *Update on the Assessment of the Removal of Social Security Numbers from Medicare Cards* (Baltimore, Md.: November 2011).

³For most individuals, the Social Security Administration (SSA) is responsible for determining eligibility for Medicare and assigning the HICN. However, for the approximately 550,000 Railroad Retirement beneficiaries and their dependents, the Railroad Retirement Board (RRB) is responsible for determining eligibility and assigning the HICN.

⁴Lynn Langston, *Identity Theft Reported by Households, 2005-2010*, NCJ 236245 (Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, November 2011).

⁵For the purposes of this statement, we define a data breach as the unauthorized acquisition, access, use, or disclosure of individually identifiable information.

involving protected health information that each affected more than 500 individuals.⁶

The importance of enhancing security protections for the display and use of SSNs has resulted in multiple actions by federal and state governments and the private sector. For example, the Social Security Administration (SSA) has advised for years that individuals not carry their Social Security card with them. In 2007, the Office of Management and Budget issued a directive to all federal agencies to develop a plan for reducing the unnecessary use of SSNs and exploring alternatives to their use.⁷ Many federal agencies, including the Departments of Defense (DOD) and Veterans Affairs (VA), have taken significant steps to remove SSNs from their health insurance and identification cards. In the private sector, health insurers have also removed SSNs from their insurance cards in an effort to comply with state laws and protect beneficiaries from identity theft. In 2004, we reported that CMS determined it would be cost-prohibitive to remove the SSN from the Medicare card.⁸ Subsequently, CMS issued a report to Congress in 2006 describing an option for removing the SSN and estimated it would cost over \$300 million to do so.⁹

Our remarks are based on our report released today,¹⁰ which describes the various options for removing the SSN from the Medicare card and examines the potential benefits, burdens, and CMS's cost estimates associated with the various options. To conduct this work, we reviewed

⁶We use the term provider to refer to any organization, institution, or individual that provides health care services to Medicare beneficiaries. These include hospitals, nursing facilities, physicians, hospices, ambulatory surgical centers, outpatient clinics, and suppliers of durable medical equipment, among others.

⁷Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (Washington, D.C.: May 22, 2007).

⁸GAO, *Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards*, GAO-05-59 (Washington, D.C.: Nov. 9, 2004).

⁹Centers for Medicare & Medicaid Services, *Report to Congress: Removal of Social Security Number from the Medicare Health Insurance Card and Other Medicare Correspondence* (Baltimore, Md.: October 2006).

¹⁰GAO, *Medicare: CMS Needs an Approach and a Reliable Cost Estimate for Removing Social Security Numbers from Medicare Cards*, GAO-12-631 (Washington, D.C.: Aug. 2, 2012).

CMS's 2011 report to Congress,¹¹ as well as supporting documentation provided by CMS. We also interviewed officials from CMS, SSA, and the Railroad Retirement Board (RRB), as well as officials at DOD, VA, and representatives of private health insurers and other stakeholders. More information on our scope and methodology is provided in the full report. Our work was performed in accordance with generally accepted government auditing standards from January 2012 to July 2012 for both the full report and for this statement.

In its November 2011 report, CMS presented three options for removing SSNs from Medicare cards. One option would truncate the SSN so that only the last four digits would appear on the card. However, the full SSN would continue to be used by both beneficiaries and providers for all Medicare business transactions. The other two options would replace the display of the SSN on the Medicare card with a newly developed identifier that CMS calls the Medicare Beneficiary Identifier (MBI). In one of these options, this new identifier would be used by the beneficiary in their interactions with CMS; however, the provider would continue to use the SSN to interact with CMS. In the other, both the beneficiary and provider would use the new identifier printed on the Medicare card and the SSN would be entirely excluded from the transaction. CMS, SSA, and RRB reported that all three options would generally require similar efforts, including coordinating with stakeholders; converting information-technology (IT) systems; conducting provider and beneficiary outreach and education; conducting training of business partners; and issuing new cards. While the level and type of modifications required to IT systems would vary under each option, the one involving use of a new identifier by both beneficiaries and providers would require somewhat more-extensive IT modifications. However, CMS has not committed to implementing any of the three options presented in its report. Nor did CMS consider other options in its 2011 report, such as how machine-readable technologies, including bar codes, magnetic stripes, or smart chips, could assist in the effort to remove SSNs from Medicare cards. CMS officials told us that they limited their options to those retaining the basic format of the current paper card, and did not consider options that they believed were outside the scope of the congressional request.

¹¹Centers for Medicare & Medicaid Services, *Update on the Assessment of the Removal of Social Security Numbers from Medicare Cards* (Baltimore, Md.: November 2011).

Of the three options presented in CMS's 2011 report, we found that replacing the SSN with a new identifier for use by beneficiaries and providers offers beneficiaries the greatest protection against identity theft. Under this option, beneficiaries' risk of identity theft would be reduced in the event that their card was lost or stolen because the SSN would no longer be printed on the card. In addition, because providers would not need the SSN to interact with CMS, they would not be required to collect or maintain this information, reducing the beneficiaries' vulnerability in the event of a provider data breach. In addition, this option presents fewer burdens for beneficiaries and providers relative to the others. Under this option, the new identifier would be printed on the card, and beneficiaries would use this identifier when interacting with CMS, eliminating the need for them to memorize their SSN or store it elsewhere as they might do under the other options. This option may also present fewer burdens for providers because they would not have to query a CMS database or call CMS to obtain a beneficiary's information to submit claims as they would with the other two options.¹² Regardless of the option, the burdens experienced by CMS would likely be similar because CMS would still need to conduct many of the same activities and incur many of the same costs. For example, it would need to reissue Medicare cards to current beneficiaries; conduct outreach and education to beneficiaries and providers; and conduct training for business partners. In addition, similar modifications to state Medicaid IT systems would be required under each option in order to process information on individuals eligible for both Medicare and Medicaid.¹³ However, according to CMS officials, the option that calls for replacing the SSN with a new identifier to be used by beneficiaries and providers would have additional burdens because of the more extensive changes required to CMS's IT systems compared to the other options.

In its report, CMS, in conjunction with SSA and RRB, estimated that altering or removing the SSN would cost between \$803 million and \$845 million, depending on the option selected. Approximately two-thirds of the total estimated costs (between \$512 million and \$554 million) are

¹²There may be some initial burdens for providers and beneficiaries under any of the three options presented by CMS. For example, according to CMS officials, some providers may be required to update their IT software and beneficiaries may be confused by any change to their identifier.

¹³State Medicaid programs are jointly-funded federal-state health care programs that cover certain low-income individuals.

associated with modifications to existing state Medicaid IT systems and CMS's IT-system conversions.¹⁴ While modifications to existing state Medicaid IT systems and related costs are projected to cost the same across all three options, the estimated costs for CMS's IT-system conversions vary because of differences in the number of systems affected, and the costs for modifying affected systems for the different options. Both SSA and RRB would also incur costs under each of the options.¹⁵ SSA estimated that implementing any of them would cost the agency \$95 million, and RRB estimated costs totaling between \$1.1 million and \$1.3 million, depending on the option.

However, we have four key concerns regarding the methods and assumptions CMS used to develop its cost estimates that raise questions about their reliability. First, CMS did not use any cost-estimating guidance when developing its estimates. CMS officials acknowledged that the agency did not rely on any such guidance, for example GAO's,¹⁶ in developing its report.¹⁷ Second, the procedures used to develop estimates for the two largest cost categories—changes to existing state Medicaid IT systems and CMS's IT-system conversions—are questionable and not well documented.¹⁸ For example, CMS's estimates for certain costs were based on data collected in 2008, at which time the agency had not developed all of the options presented in the 2011

¹⁴CMS would incur \$261 million as the federal share of the estimated total of \$290 million. The remaining \$29 million would be the responsibility of the states.

¹⁵Both SSA and RRB perform Medicare-related activities and would need to make changes to their business processes and IT systems as a result of any of the options to remove SSNs from Medicare cards. SSA determines Medicare eligibility for persons who receive or are about to receive Social Security benefits, enrolls those who are eligible into Medicare, and assigns them a HICN. Though CMS prints and distributes the Medicare card, beneficiaries often contact SSA when they need a replacement card. RRB is responsible for determining Medicare eligibility for qualified railroad retirement beneficiaries, enrolling them into Medicare, assigning HICNs to these individuals, and issuing Medicare cards to them.

¹⁶GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Cost*, GAO-09-3SP (Washington, D.C.: March 2009).

¹⁷CMS developed its estimates in conjunction with SSA and RRB by examining cost categories that included potential modifications to IT systems, reissuance of Medicare cards, and beneficiary outreach and education.

¹⁸In addition to Medicaid IT-system modification costs, this cost category includes related costs, such as business-process changes, training, and updates to system documentation.

report.¹⁹ In addition, while CMS asked for cost data from all states, it received data from only five states—Minnesota, Montana, Oklahoma, Rhode Island, and Texas—and we were unable to determine whether these states are representative of the IT-system changes required by all states. For CMS's own IT systems, cost estimates for required modifications were approximately three times higher than those in the agency's 2006 report.²⁰ CMS could not explain how or why a number of these systems would be affected under the three options. Officials also could not explain the variance in the costs to modify these systems across the options and could provide only limited documentation on the development of CMS's estimates. Third, we identified inconsistencies in some assumptions used by CMS and SSA in the development of the estimates. For example, CMS and SSA used different assumptions regarding the number of Medicare beneficiaries that would require new Medicare cards. Fourth, CMS did not take into account other factors when developing its cost estimates. For example, CMS did not consider possible efficiencies that could be realized by combining IT modifications required to remove SSNs with related IT modernization efforts. The agency also did not attempt to calculate potential savings due to the reduced need to monitor compromised SSNs if they were removed from Medicare cards.

In conclusion, nearly six years have passed since CMS first issued a report to Congress that explored options for removing the SSN from the Medicare card, and five years have elapsed since the Office of Management and Budget directed federal agencies to reduce the unnecessary use of the SSN. While CMS has identified various options for removing the SSN from Medicare cards, the agency has not committed to a plan for such removal. Lack of action on this key initiative leaves Medicare beneficiaries exposed to the possibility of identity theft. Therefore, we recommended that CMS select an approach for removing the SSN from the Medicare card that best protects beneficiaries from identity theft and minimizes burdens for providers, beneficiaries, and

¹⁹CMS officials told us that the new identifier for beneficiary use and new identifier for beneficiary and provider use options had already been developed at the time CMS requested data from the states, but the agency did not include the truncation option when it requested data from the states.

²⁰In its 2006 report to Congress, CMS estimated that removal of the SSN from Medicare cards would cost approximately \$338 million, of which \$80.2 million was attributable to start-up costs for IT-system modifications.

CMS; we also believe CMS should develop an accurate, well-documented cost estimate for such an option using standard cost-estimating procedures.

In responding to a draft of the report on which this testimony is based, CMS concurred with our first recommendation to select an approach that best protects beneficiaries from identity theft while minimizing burdens for beneficiaries and providers. CMS also concurred with our second recommendation, stating that it would conduct a new estimate and utilize GAO's suggestions to strengthen its estimating methodology. SSA, RRB, and DOD, had no substantive comments and did not comment on the report's recommendations. VA concurred with our findings.

Chairman Johnson, Chairman Herger, and Members of the Subcommittees, this completes our prepared statement. We would be pleased to respond to any questions you may have at this time.

If you or your staff have any questions about this testimony, please contact me at (202) 512-7114 or kingk@gao.gov, or Daniel Bertoni at (202) 512-7215 or bertonid@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are listed in appendix I.

Appendix I: GAO Contacts and Staff Acknowledgments

GAO Contacts

Kathleen King, (202) 512-7114 or kingk@gao.gov, or Daniel Bertoni, (202) 512-7215 or bertonid@gao.gov.

Staff Acknowledgments

In addition to the contacts named above, the following individuals made key contributions to this statement: Lori Rectanus, Assistant Director; Thomas Walke, Assistant Director; David Barish; Carrie Davidson; Drew Long, and Andrea E. Richardson.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."
Order by Phone	<p>The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.</p> <p>Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.</p> <p>Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.</p>
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov .
To Report Fraud, Waste, and Abuse in Federal Programs	<p>Contact:</p> <p>Website: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470</p>
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov , (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov , (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548



Please Print on Recycled Paper.

Chairman JOHNSON. Thank you, ma'am. I thank you both for your testimony. We will now turn to questions.

And as is customary for each round of questions, I will limit my time and will ask my colleagues to limit their questioning time to five minutes, as well.

Mr. Trenkle, do you speak for CMS?

Mr. TRENKLE. Do I speak for CMS?

Chairman JOHNSON. Yes. Can you make a statement on their behalf?

Mr. TRENKLE. I can certainly make statements on their behalf to some extent. Obviously, I am a career employee of CMS; I am not a political employee. So I can only speak at a certain level.

Chairman JOHNSON. Well, that shouldn't matter. On behalf of the one million Medicare beneficiaries, I am a little bit upset. First, CMS responded to a bipartisan letter from leadership of this committee over 12 months after the deadline. And I think it is unfair. But how dare CMS treat this committee, this Congress, and our nation's seniors with such contempt?

Second, despite the fact that this committee's bipartisan letter asks for detailed estimates and justifications for all costs, we now learn from GAO that your cost estimates aren't credible.

Finally, despite a decade of instruction from the Congress to take Social Security numbers off Medicare cards, CMS has not committed to a plan for such removal. And you are probably aware that the health organizations around the country took them off, and that the military has been taking them off.

Mr. TRENKLE. Right.

Chairman JOHNSON. And if they can do it, and you were asked to do it some many years ago, I don't understand what is taking so long.

In your testimony you say CMS takes seriously the risk of identity theft for Medicare beneficiaries, and that it appreciates the concerns expressed by Congress, and beneficiaries, regarding the continued use of serial numbers on Medicare cards. Do you believe this?

Mr. TRENKLE. Yes, I do. I can certainly understand your frustration and other frustrations of the committee and subcommittees regarding where we have gone over the last seven years with the two cost estimates and the other work that is being done by federal agencies.

Chairman JOHNSON. Well, it is all of us, both the Democrats and Republicans working together on this committee that have become upset about empty words. And it is outrageous that you are kind of thumbing your nose at Congress and seniors.

I can only conclude that CMS is busy doing other things besides protecting the privacy of seniors and the integrity of Medicare. So, it seems it is going to take an Act of Congress—another one; we already made one—to make CMS remove the Social Security numbers.

Mr. Trenkle, is it true that CMS requires that cards issued by Part C, Medicare Advantage, and Part D, prescription drug benefits, do not display a Social Security number?

Mr. TRENKLE. Yes, that is correct.

Chairman JOHNSON. Aren't you being hypocritical, asking your service providers to do what you won't do?

Mr. TRENKLE. I don't believe it is hypocritical. I think, as part of the changes in the OMB directive, we made a number of changes over the last several years. That was one that we—as we implemented the Part C and D plans, that we made that change. And, as you say, that was done by the private insurers.

However, to do something on the scale of what we are talking about for CMS and Medicare, we are talking about a much larger effort that is much more intertwined with other federal agencies.

I mean the Medicare Advantage is probably about 25 percent of the overall Medicare. So if we are talking, say, 50 to 52 million Americans, that is 13 million, as opposed to 39 million, plus the connections with SSA—

Chairman JOHNSON. Well, let me just interrupt you and say GAO talks about the Department of Defense and Veterans Affairs efforts to remove the Social Security numbers from their ID cards. Have you even talked to them to find out how they did it?

Mr. TRENKLE. We have talked to them, and we have also talked to the private insurers, as well.

It is good to keep in mind—and I am not—let me just first state up front I am not making excuses. I certainly want to work with Congress, and we want to work with you all to look at the various priorities that Congress has asked us to do, and see how we can work this in with the other priorities for the Medicare program. So I don't want to make excuses.

But I do want to say that there are differences between the DoD and VA. One is the scale; our scale is much larger. The second is that VA is a closed system. DoD is a partly closed health care system. So—and they are certainly not as entwined with Social Security.

If you remember, Social Security really works as our arm of operations for this program. So it is not to trivialize the work that they have done, but just to say that it is going to be a massive undertaking if we go down this road.

Chairman JOHNSON. Well, they did it because they were able to and willing to make the change as they print new cards. You print new cards in millions. And I don't understand why we can't get something going. It has been too many years behind.

And I will stop there and question some more later. And I yield to my compadre, Mr. Becerra.

Mr. BECERRA. Mr. Chairman, thank you. And thank you to the three of you for your testimony. And I hope that this is just the beginning of a process to get us to the point where we are able to remove that Social Security number from the Medicare cards.

Mr. Trenkle, let me ask a couple of questions. In terms of the implementation of the different services that CMS and Medicare provide to the millions of Americans who are beneficiaries of Medicare services, having paid into the system to earn those benefits, Medicare doesn't have any local offices to administer the services that seniors and others who receive Medicare benefits need. Right? They don't have their—

Mr. TRENKLE. That is correct.

Mr. BECERRA. When a senior applies for Medicare, that senior doesn't go to a Medicare office, but he or she must go to a Social Security office. Is that correct?

Mr. TRENKLE. That is correct.

Mr. BECERRA. That means that taking in an application for benefits, or responding to inquiries regarding Medicare benefits is done—if it is done directly to an office, it is done to a Social Security office.

Mr. TRENKLE. That is correct.

Mr. BECERRA. Who issues Medicare cards?

Mr. TRENKLE. The cards are—the numbers are actually—SSA actually does the enumeration, and we actually issue the Medicare cards.

Mr. BECERRA. So, Social Security is part of the process of issuing these cards to seniors, the Medicare cards?

Mr. TRENKLE. That is correct, except I also want to mention in the case of the Railroad Retirement Board, they actually do it for the Railroad Retirement Board retirees and—

Mr. BECERRA. And if a senior needs to have a Medicare card replaced, they go to a Social Security office.

Mr. TRENKLE. That is correct.

Mr. BECERRA. Okay. Who collects the premiums, the Medicare premiums, from seniors?

Mr. TRENKLE. It is part of the Social Security—it comes out of the Social Security check.

Mr. BECERRA. And if a senior wants to talk to someone in person, has a question about his or her Medicare benefits and wants to speak to someone in person, they are confused about their benefits, they don't believe they got their correct service out of Medicare, they go to a Social Security office, do they not?

Mr. TRENKLE. That is correct.

Mr. BECERRA. So while I know you are here with CMS and not with the Social Security Administration, it is clear that the Social Security Administration will have a large role to play in whatever we do with removing the Social Security number from the Medicare card.

Mr. TRENKLE. Yes, that is correct. And as I mentioned earlier in my testimony, I worked at both places, so I understand that the—impact this will have on the field offices at Social Security.

Mr. BECERRA. And while we are hoping to get a more accurate estimate of the cost of removing that number from the Medicare card, it is clear that it is going to cost some money.

Mr. TRENKLE. That is correct.

Mr. BECERRA. And there—we have got estimates. Early estimate in 2005, 2006 was somewhere over \$300 million.

Mr. TRENKLE. That is correct.

Mr. BECERRA. A 2011 estimate was somewhere over \$800 million. We are talking in the hundreds of millions of dollars, likely, to remove the card and secure the safety of that—excuse me, remove the Social Security number from the card and to secure the safety of that number for our Medicare beneficiaries.

Mr. TRENKLE. That is correct. And also, there is going to be considerable outreach required, because of the fact that we will need to educate the beneficiaries and their families on the changes that are being made to that card, as well as the provider community. The provider community, this will be a major change for them, as well.

Mr. BECERRA. So this is not something that the Social Security Administration or CMS, which helps administer Medicare, currently is being funded to do.

Mr. TRENKLE. That is correct.

Mr. BECERRA. And so, either you receive resources to try to compensate for the hundreds of millions of dollars it will cost to

make this change to secure the Social Security number for seniors on their Medicare card, or you have to shift your resources from other current services in order to pay for the cost of this transition.

Mr. TRENKLE. Yes, that is correct.

Mr. BECERRA. What types of services might be affected if you have to take from existing resources and—existing services in order to cover the cost of transitioning to a Medicare card without a Social Security number?

Mr. TRENKLE. Well, I can't really speak to that today, because part of it is—as you know, most of the work that we do is based on congressional legislation, and we follow out the wishes of Congress. So if we are going to make some changes and it would impact priorities, we would need to work with you and others and determine which priorities would need to be shifted to enable us to fund that out of our existing resources.

Mr. BECERRA. Well, I hope you are able to give us some clear guidance on what might happen if we instruct CMS and Social Security and Medicare programs under HHS to move forward with this transition without providing you with the resources. Because I can assume that it can only get worse for seniors who are right now trying to get their Social Security services. They have already seen, as a result to the budget cuts to Social Security Administration's budget, reduction in the number of hours that their offices are open. There are longer wait times now when people call the 1-800 number to get Social Security services. We understand that the Social Security Administration has had to reduce the size of its staff.

And so, more and more, what we are talking about is short-changing Americans who work very hard to pay for their Social Security and Medicare services. And I would hate to see that we instruct you to do something that is absolutely essential to provide protection against identity theft, but we do at the cost of providing good service to those who worked so hard to earn those services.

So, I thank the three of you for your testimony. I look forward to working with you in the future.

Mr. TRENKLE. Thank you.

Mr. BECERRA. Thank you, Mr. Chairman. Yield back.

Chairman JOHNSON. Thank you. Chairman Herger, you are recognized for five minutes.

Mr. HERGER. Thank you, Chairman Johnson. And, Mr. Trenkle, I am pleased to hear that under questioning from Chairman Johnson you indicated that you are not here to make any excuses.

More than one decade ago, GAO first recommended removing Social Security numbers from government documents. CMS failed to act. More than five years ago the OMB issued a directive telling all federal agencies to develop a plan for reducing unnecessary use of Social Security numbers and explore alternatives. Again, CMS failed to act.

Now, I know CMS claims that Social Security numbers are important to carrying out program functions. But I have to imagine it was also important to the DoD, the VA, and they are well on their way to removing Social Security numbers. I also imagine it was important to private insurance companies before they removed Social Security numbers, replacing them with unique identifiers. I

am sure the same can be said for Medicare Advantage and prescription drug plans.

The Social Security Administration inspector general states, “Medicare cards unnecessarily place millions of individuals at risk for identity theft. We do not believe a federal agency should place more value on convenience than the security of its beneficiaries’ personal information.”

After more than 10 years, CMS has failed to lead and failed to act. And, as a result, nearly 50 million Americans are at risk. In fact, were it not for a directive from Congress, I wonder if CMS would have even considered removing Social Security numbers from the Medicare card.

Mr. Trenkle, does this Administration believe Social Security numbers should be taken off of the Medicare identification cards to protect our seniors?

Mr. TRENKLE. Thank you, Chairman, for your remarks. And as I said earlier to Chairman Johnson, I understand your frustration. And I—

Mr. HERGER. And if you could give me a yes or no, does the Administration feel the numbers should be taken off?

Mr. TRENKLE. As I mentioned earlier, we do feel that the option one that GAO spoke of, which was replacing the number with a new identifier, would offer the greatest protection against identity theft.

Mr. HERGER. Then why hasn’t CMS acted?

Mr. TRENKLE. Well, as I mentioned a few moments ago, we have a number of congressional mandates around the Medicare program that we are trying to implement. And this will be an extensive undertaking, regarding of how you look at the cost numbers. It will be an extensive undertaking. So we need to work with you and others in Congress to reprioritize, or look at the other priorities, to determine how this will be taken care of, if additional appropriations are not given to us for this.

Mr. HERGER. And, Mr. Trenkle, are you aware that the Department of Defense and Veterans Administration did not require new funding to remove Social Security numbers from their membership cards? They use existing funding?

Mr. TRENKLE. I heard that this morning, and I am not really aware of how they did the change and how they made the necessary budget adjustments to do that. So I would certainly be interested in talking to them more about how they managed to do that within their existing budgets.

Mr. HERGER. Now, I know that Medicare has far more beneficiaries, but I also know that CMS administrative budget is quite large. Why is it that CMS can’t follow in the footsteps of DoD and VA, and use existing money to implement this long overdue and needed change?

Mr. TRENKLE. Well, as I said earlier, it is not exactly comparing apples to apples, because they do have a different type of setup, in terms of the—how its—how the operations are done, that they operate mostly within closed systems, and that they have different types of arrangements, in terms of funding, than we do. So I can’t say they can do it this way and we can do it that way.

But at the same point, I understand what you are saying. It is a large budget, and we do an awful lot of work with that budget, as you know, because a lot of legislation comes out of Congress each year that impacts us.

So, as I have said earlier, we will commit to looking at that in our new and more rigorous cost estimate, and see where there—if we cannot get additional appropriations, how we can work with Congress to reprioritize some of the mandates that you have asked us to achieve.

Mr. HERGER. And I might just close with how can you expect Congress to provide additional funding when your agency, according to GAO, is unable to produce a credible estimate?

And I yield back.

Chairman JOHNSON. Thank you. Mr. Stark, you are recognized.

Mr. STARK. Thank you, Mr. Chairman. I want to thank the panel for their enlightenment this morning.

The—Mr. Trenkle, I guess GAO has had two recommendations. And what—which one would—approach would you prefer for removing the Social Security numbers?

Mr. TRENKLE. I guess I mentioned that just a moment ago, that we think that the one that would provide the best—we would like to re-estimate all three options, but the one that we feel that would provide the best protection against identity theft would be replacing the number with a new number, which is our option one.

Mr. STARK. Could you state today a timeline, an estimate within a couple of months, one way or the other, as to what it would take to complete this—the contractor, and have it completed?

Mr. TRENKLE. To re-do the estimates? I think we could do that within the next six months. Certainly without—let me—

Mr. STARK. Yes.

Mr. TRENKLE. The only caveat would be the Medicaid costs, which may require more research to make sure that we have them correct. But I think we can leverage the work we have already done, do the more rigorous cost estimating work with our colleagues from GAO, and bring another contractor. I feel that we can do that within the next six months.

Mr. STARK. Great. Thank you very much.

Mr. TRENKLE. Thank you.

Mr. STARK. Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Mr. Stark. Mr. Reichert, you are recognized.

Mr. REICHERT. Thank you, Mr. Chairman. Mr. Trenkle, have you been a victim of identity theft?

Mr. TRENKLE. I have not, personally, although I know others who have.

Mr. REICHERT. So you have visited with people who have been victims of identity theft?

Mr. TRENKLE. I know people who have been victims of identity theft, and it is not a trivial matter that it happens, yes.

Mr. REICHERT. Have you had an opportunity to visit with some of the constituents that you serve through your job, current job, regarding identity theft and the impacts on American citizens?

Mr. TRENKLE. The ones who have had identity—have had—have been victims of identity theft?

Mr. REICHERT. Yes. Have you had the opportunity to visit with any of the beneficiaries who have been victims?

Mr. TRENKLE. Not personally, no.

Mr. REICHERT. So when you say you understand the concerns, what are you—I don't know what you really understand about identity theft.

I was a police officer for 33 years, and I dealt with people who lost their identity. And it was one of those events that can be traumatic enough to turn your life upside down. Lose your home, lose your car, lose your—everything you own.

So, do you believe that it—10 years has been mentioned. Personally, do you believe that is—you should have had this solved by then, by now, 10 years later? Or—I mean do you think that is too long, or do you think you are just about in the ballpark where you need to be, or—

Mr. TRENKLE. Well, let me—

Mr. REICHERT. I just was wondering personally how you felt about—I mean you are a part of the system. Ten years to solve this problem. I am just wondering how you personally feel about having worked on this—you feel some frustration?

Mr. TRENKLE. I understand your frustration.

Mr. REICHERT. No, I am asking you if you feel frustration.

Mr. TRENKLE. Right. Yes. Yes.

Mr. REICHERT. What is the sort of the—what happens to you or other members of CMS if they don't accomplish this task? What is the hammer? What is the outcome for you? I mean you get to work every day. You get your job, right?

Mr. TRENKLE. Right.

Mr. REICHERT. What is the outcome for Americans if you don't get it done? They become victims of identity theft and they lose their homes.

Mr. TRENKLE. Well, I think—

Mr. REICHERT. What is your motivation to get this accomplished?

Mr. TRENKLE. The motivation to get it accomplished is that I feel that it is one of the potential ways that there can be identity theft. There is much more ways of that happening than through the Medicare card. And we are here to serve the Americans every day, not only because I have family members, but because I—

Mr. REICHERT. If I could—Mr. Trenkle, 10 years.

Mr. TRENKLE. Yes.

Mr. REICHERT. The American people don't understand why it takes 10 years to accomplish this. And what I hear from you—and I—you know, your statement about congressional mandates, and we need to reprioritize congressional mandates, can you be specific about what those mandates—what kind of mandates are you talking about?

Mr. TRENKLE. Well, there is many changes to the Medicare—

Mr. REICHERT. For example?

Mr. TRENKLE. For example? There is changes in payment schedules that occur each year. There is changes in—

Mr. REICHERT. Those are congressional mandates, or that is just part of your daily routine?

Mr. TRENKLE. Often changes in—yes.

Mr. REICHERT. Are the congressional mandates that you are speaking about, are they associated with the new health care law that we are in the middle of implementing?

Mr. TRENKLE. That is certainly one of the congressional mandates, yes.

Mr. REICHERT. So how could we alter the current health care law to help you keep Americans from suffering the victimization that identity theft brings? How can we change this implementation process to help you get that done?

Mr. TRENKLE. Well, as I said earlier, I am happy to work—
Mr. REICHERT. Just one idea?

Mr. TRENKLE. I am not really—I really don't—

Mr. REICHERT. Mr. Chairman, I yield back.

Chairman JOHNSON. Thank you. You know, how many millions of cards do you produce a year?

Mr. REICHERT. We produce millions of cards a year. I could get you the number.

Chairman JOHNSON. It is close to three million, I think.

Mr. REICHERT. Yes, it—well, it is actually higher than that now. And about 10 percent of them are actually—have to be replaced each year, either because they are lost, or because there is other reasons why. Someone changes their name, or—

Chairman JOHNSON. Yes. Well, you see, the Defense Department solved this issue by putting a new number on the new cards they issue. Why in the world can't you guys do that?

Mr. TRENKLE. It can be done. That is one option.

Chairman JOHNSON. Well, why haven't you done it?

[No response.]

Chairman JOHNSON. I mean I don't think you guys are into this issue like you should be, to protect the United States citizen. Wow.

Mr. McDermott, you are recognized. What, did he leave? Oh, wake up down there.

[Laughter.]

Mr. MCDERMOTT. I didn't think you would jump past all those worthies down there.

Chairman JOHNSON. Thank you.

Mr. MCDERMOTT. Do you know that there is an election some—are you aware of that?

Mr. TRENKLE. I have heard something about that.

Mr. MCDERMOTT. And occasionally there are hearings that sort of strike one to be a little bit political. I—we have nine legislative days left, so I don't know if we are going to get down to this. But I was trying to figure out practically, following up on those last questions, there are 50 million people participating in Medicare. Now, it shouldn't take you much more than a week to print 50 million cards and put them in envelopes and send them on out to these people. Should it?

Mr. TRENKLE. Well, it would probably take a little bit longer than that.

Mr. MCDERMOTT. Well, let's say a month. Let's say a month. I mean that is—we do political campaigns and we send out millions of pieces of information to folks. And you could just put it in an

envelope and send it on out. So you could send out 50 million in a month. Or maybe two months. Let's do it that.

Now, what kind of chaos do you think that would create in the system for the providers? Because I am looking at it—I hear Mr. Reichert talk about he is a police officer. I am a doctor. So now I got all these seniors coming in. What kind of chaos are you going to create for the providers by putting out 50 million new cards and new numbers to put on all the forms?

Mr. TRENKLE. It would create quite a substantial change for the providers. There is no doubt about that.

Mr. MCDERMOTT. So you think that the chairman is thinking about the providers when they are talking about changing this number? Do they just think this is something—they are only thinking about the seniors' votes, but not the providers' votes when this chaos is created?

Mr. TRENKLE. I can't speak for the chairman. I don't know. I do know that will be an impact on—that certainly will be a major impact on the providers.

Mr. MCDERMOTT. How does that number get—I mean how does the doctor get the number that he is supposed to put on the form?

Mr. TRENKLE. Gets it from the card.

Mr. MCDERMOTT. And so, if these 50 million members now have a new card, and they have got to bring it into their doctor and say, "Doctor, here is my new number, don't put that old number, you won't get paid," right, how many—what would you just guess is the percentage that would not get that number in, or wouldn't have the card in their pocket when they got sick or got hit by a car, or whatever?

Mr. TRENKLE. Oh, I can't even estimate that.

Mr. MCDERMOTT. But it would—you would suspect there would be a sizeable number of people.

Mr. TRENKLE. It would certainly have the potential to impact a great number of people, yes.

Mr. MCDERMOTT. You know, I refinanced my house the other day. And the lady on the phone said, "Give me the last four digits of your Social Security number." Now, are the banks allowed to use that as an ID number?

Mr. TRENKLE. Yes, they do that quite often with the last—

Mr. MCDERMOTT. The banks can do it.

Mr. TRENKLE. Yes.

Mr. MCDERMOTT. Well, why don't you give me a special number so I can have my American number, so I can give that to them and get rid of that Social Security number so nobody can find out what I am doing?

I mean you are going to keep a record of these numbers, right?

Mr. TRENKLE. Correct.

Mr. MCDERMOTT. And so I—instead of having 358-28-7705, I am going to have 779-16-4382. Right?

Mr. TRENKLE. That is correct.

Mr. MCDERMOTT. Somewhere, that list will be with that—right?

Mr. TRENKLE. Yes.

Mr. MCDERMOTT. How do these people lose their identity? How does somebody get my number and pull it out and start fiddling with my financial stuff at the bank?

Mr. TRENKLE. I don't feel qualified to speak to all the ways that identity can be compromised. There are certainly a number of ways it can be compromised.

Mr. MCDERMOTT. Does your fraud division use—does the CMS fraud division use that Medicare number?

Mr. TRENKLE. Yes, they do.

Mr. MCDERMOTT. So we got to make sure we get this to them so they can trace these fraudulent operators who are operating these places down in Florida and Texas, where they are just rolling in dough with people who aren't receiving benefits. You need a number for those kind of fraud investigations.

Mr. TRENKLE. That is correct.

Mr. MCDERMOTT. So this number, this new number, I am going to be carrying a card in my pocket with it on it. Right?

Mr. TRENKLE. Correct.

Mr. MCDERMOTT. Presumably.

Mr. TRENKLE. Presumably, yes.

Mr. MCDERMOTT. I mean I have my—I was looking here at my Medicare—or my cards here from my insurance from the legislature, from the Congress. And I have got a number on there. It is not my—it is not that old Social Security number, but it is a number. So somebody can get a number for me and plug in some way—I understand there is people who hack into computers. Is that right?

Mr. TRENKLE. I have heard of a few who have, yes.

Mr. MCDERMOTT. Have any of them gone to jail?

Mr. TRENKLE. I presume so, yes.

Mr. MCDERMOTT. Have some of them taken money out of Medicare?

Mr. TRENKLE. Yes.

Mr. MCDERMOTT. So they hacked into a computer where there was a list of numbers, right?

Mr. TRENKLE. I really can't—I don't feel like I can really get into a whole lot of detail on that subject. But I mean there is certainly possibilities for hackers to get into systems of any organization. I mean—

Mr. MCDERMOTT. Do you think it is possible in this electronic world we have today to give people 100 percent certainty that they are not going to lose their identity through this method?

Mr. TRENKLE. No, I don't believe so.

Mr. MCDERMOTT. I yield back the balance of my time.

Chairman JOHNSON. Thank you. The gentleman's time has expired.

Mr. STARK. Mr. Chairman.

Chairman JOHNSON. Yes?

Mr. STARK. Yield for a second to ask the gentleman from Washington?

If you—when Bubbles sends you that email and asks if you want a good time and just send her your Social Security number, if you don't do that, then she won't have your Social Security number. Okay?

[Laughter.]

Chairman JOHNSON. I am not sure I understood that. But Mr. Berg, you are recognized.

Mr. BERG. Well, thank you, Mr. Chairman. You know, one of the things that we do is we learn from other agencies and how they have gone through this. You know, as we sit here and listen to the frustration, I, you know, go back to 2002, I think, when GAO first came out and made this recommendation.

Really, Mr. Bertoni, if we could kind of get to, you know, what steps DoD took and the VA to remove Social Security numbers from the membership cards, and tell us, you know, what those agencies do well. Is there anything that Medicare can learn from this and implement, as we are here today?

Mr. BERTONI. I think, first and foremost, they recognized it as a priority. And whether it be in response to directives from the outside, or just the basic cultural shift in this country, that we need to remove SSNs from massive use and display and then move forward in trying to use appropriate technology in house—I mean within their budget—to redact and remove these SSNs.

So, the first step was to get them off the cards. So I would say that was a great effort. Now these SSNs and other information are embedded in the mag strips and the bar codes behind—within the card. The agencies, both DoD and VA, are realizing that that is first generation technology, and they are already looking forward to what they need to do to further protect that card, which is to remove the SSN information and replace it with a non-SSN-based identifier. So, clearly, CMS is—if they move forward, we prefer it to head in that direction. So that is a lesson learned. You want to get the card—the number off the front, and off any bar code or mag strip or anything in the card.

Certainly DoD piggy-backed off of existing IT adjustments. They were able to leverage resources to make the changes in accordance with other adjustments. So I think that would be—CMS might want to talk to them about.

And lastly, I think this cost is high in some respects because it is a rapid-phase-in. It is a one-year period. They are going to run dual systems for one year. But after that it is going to go to a single system, and they are going to have all these people issued new cards. There may be some opportunities to leverage resources to look at, if they ran dual systems for the second year or third year, would that counteract any additional costs that they are claiming would be encountered if they ran dual systems for more than a year. I don't know if that analysis has been done. I think they could reach out to DoD and VA to see how that worked and what the cost savings were.

Mr. BERG. Well, thank you. And that is really my only question we have part of the same family here. Let's use the best practices and implement them.

I will yield back, Mr. Chairman.

Chairman JOHNSON. Thank you. Appreciate that. Mr. Doggett, you are recognized.

Mr. DOGGETT. Mr. Chairman, thank you. And I want to express my full agreement with the comments that you have made here this morning, and that you have made here in the past concerning

this very serious matter of identity theft, and the failure of CMS to live up to its responsibilities to address it.

This is not a matter of frustration. It is a matter of the proper oversight of this committee over the actions of CMS. We have had bipartisan agreement about the severity of this problem and the need to address it. And we have also had bipartisan inaction at CMS. This began during the administration of President Bush. It has continued under the administration of President Obama. Under neither administration has CMS been responsive on this matter.

When we together, Mr. Chairman, introduced the legislation that Congress passed way back in 2008, it was not a smooth process. CMS resisted in every way our approval of that legislation. And to address the concerns that CMS voiced then about the legislation, we amended it to provide that they did not have to achieve all aspects of this until necessary appropriations were made available. They came in with what I considered at that time—and this was under the Bush Administration—an estimate that was very high, as we were about to get the legislation passed, as a way to discourage approval of the legislation.

The problem is that CMS never agreed that this was a priority, or that it needed any attention. They didn't agree with what I think was the very proper recommendation of the Office of Management and Budget under the Bush Administration. The CMS part of the bureaucracy didn't think it was something that needed to be done. We finally got it passed after it was delayed here in the House until very near the end of the session. And the continued resistance of CMS managed to get this bill stopped in the Senate.

Since that time—the reason we have a GAO report today in the first place is that we gave up on trying to get a straight answer from CMS as to the basis for their cost estimate. And it—finally, in desperation, we turned to the Government Accountability Office to try to get a straight answer. And now, years later, all we find out really is it will cost some money, and we don't have a straight answer.

And if I understand your testimony this morning, Mr. Trenkle, you are saying that in another six months you are going to contract out with someone else to do the estimate that my office started trying to get from you back in about 2007 or 2008? Is that what this contract is about?

Mr. TRENKLE. We will use a contractor to help support the effort.

Mr. DOGGETT. Well, I guess I can't argue, after all this time, that maybe we are going to get a straighter and more complete answer from a contractor than we have gotten from CMS.

But the notion that this morning CMS thinks that, well, maybe after all these years it is time to talk to DoD or VA about how they accomplished it without spending \$800 million, and get an accurate estimate, I find truly amazing that it would—that at this late date, years later, we would have no plan, no ability to estimate internally what the cost will be that is credible, and now we are going to spend money to have some outside source tell us what we should have been told at the time that Chairman Johnson and I introduced this legislation back in 2007 or 2008.

I believe, Mr. Chairman, that until we go ahead and pass legislation on this, we are not going to get the action that is necessary. I don't agree with Chairman Herger, that this has anything to do with the Affordable Health Care Act, because it has been going on so long, and the unresponsiveness has been so consistent between administrations, that I think it takes some congressional action. I don't believe that this can be done for free. There are some appropriations that will be necessary. But those appropriations have to go hand in hand with a new attitude that is more responsive about the severity of this problem than we have had over the course of the last decade.

And I yield back.

Well, if I might, Mr. Chairman, if I still have a moment, let me just ask the folks, Ms. King and Mr. Bertoni, do you—were you able to get any indication, even if they did it within their existing appropriations, of what this costs to do at either the VA or the Department of Defense?

Ms. KING. We did ask them that. But we are not totally confident of the answer, because it is not a process that we looked behind to verify.

Mr. DOGGETT. There were some costs associated with it.

Ms. KING. Yes.

Mr. DOGGETT. But they accommodated this on a gradual basis, and as they were making some other technology changes.

Ms. KING. Yes.

Mr. DOGGETT. I guess it is hard to break it down.

Ms. KING. Yes.

Mr. DOGGETT. Thank you very much.

Chairman JOHNSON. Well, that is true. But they also replace those cards periodically, too. But so does CMS.

Looks like Mr. Berg is gone, so how about—yes, Mr. Gerlach, you are recognized.

Mr. GERLACH. Thank you.

Chairman JOHNSON. Yes, sir.

Mr. GERLACH. Mr. Trenkle, I am really stunned, too, by the lack of responsiveness by CMS on this issue over the years, to follow up on Mr. Doggett's commentary.

Can you give us a concise and specific explanation for that lack of responsiveness beyond your testimony that just says, "given the budgetary and logistical challenges of removing Social Security numbers." Can you give us more specificity and conciseness as to why there is this internal, departmental lack of responsiveness to the need to do this?

Mr. TRENKLE. I don't think there is a lack of responsiveness to do this. I personally have only been involved in this for the past year.

But I think there is other—as I said before, there is other priorities that we are dealing with in the Medicare area. And that has been where we have been looking at over the past two cost estimates. People have looked at the costs and have looked at other priorities, and have said that this will take a significant number of resources, time, and effort to do.

Mr. GERLACH. How much money do you think would be saved in savings from improper payments that occur within the system,

which is—the GAO has estimated in this most recent report \$48 billion a year of improper payments in Medicare each year—how much of that \$48 billion can be saved if there is more security around the beneficiaries' cards, their identification, their identity? How much can be saved if this were fully implemented?

Mr. TRENKLE. I am not prepared to answer that question.

Mr. GERLACH. Why not?

Mr. TRENKLE. Because the—

Mr. GERLACH. Why haven't you estimated that? Congress has told you repeatedly, year after year, that this has to be done. And there is tremendous savings that would result from it. Why haven't you figured out what that number is?

Mr. TRENKLE. As I—

Mr. GERLACH. Do you care? Do you really care about saving the identity and the taxpayer's funds that go into this program? Do you really care?

Mr. TRENKLE. Yes, I care, and—

Mr. GERLACH. Then how do you demonstrate it? You are the Office of Information Services. In your request to your superiors for this year's budget, you make a request from your office to your superiors that ultimately winds up through OMB, that then becomes part of the President's request to Congress. Have you asked for a specific line item in your budget that you can use to go out and implement this program?

Mr. TRENKLE. Well, the budget includes more than IT. It includes other costs.

Mr. GERLACH. Have you requested from your office to your superiors, "Give me X number of dollars this year, so I can implement this program immediately"?

Mr. TRENKLE. No, I have not.

Mr. GERLACH. Why?

Mr. TRENKLE. As I—

Mr. GERLACH. You know Congress wants to get this done. Why haven't you done that?

[No response.]

Mr. GERLACH. You don't care, obviously. Until you put in writing what you want to do, "This is my priority, I am in charge of this office of information services, Congress needs to get this—wants us to get this done, we need to get it done, here is my request for that amount of money, let's get it done," you obviously don't care.

So, the next question is when are you going to start caring? Will this hearing help you start caring? That is a yes or no answer. Will this hearing help you start caring?

Mr. TRENKLE. Well, as I say, we are going to go back and do the re-estimate and work with Congress to reprioritize if there needs to be—this needs to be done, and if we don't get additional appropriations.

Mr. GERLACH. You don't need additional appropriations, necessarily. You haven't even identified how much money you really need to start the process. And, therefore, how do you know if you have it or not within your budget?

And if you do think you need extra money, where is the request of this—to this Congress for that money?

[No response.]

Mr. GERLACH. Well, obviously, I am frustrated. I apologize for how I have questioned you today. I usually don't question witnesses in this manner. But hopefully you can understand how frustrated many of us are. And if you don't have the resources needed to get this done as soon as possible, I hope you will talk to your superiors at CMS to create a special line item request in your next budget proposal to make this happen. Do I have your assurance you will do that?

Mr. TRENKLE. As we do the new estimate, that is certainly something that I can talk to our leadership at CMS about.

And I do understand your frustration and others. I know this has been a process that has occurred over many years. And hopefully, at this point, with the new estimate, we can move forward to work with you and others to prioritize this along with other priorities.

Mr. GERLACH. All right. Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you. It might not cost anything, if you take a good look at it.

Mr. Pascrell, you are recognized.

Mr. PASCRELL. Mr. Trenkle, you would have to agree that it gets frightening and weird and scary when both sides agree in this Congress.

[Laughter.]

Mr. PASCRELL. Holy mackerel. I looked up both the CMS budget over the last four years, five years, and Social Security Administration budget. And not only have we flatlined it, but there have been hiring freezes—there has been in many agencies. Social Security, I think, closed 300 small field offices. When you look at both of these agencies, which will be intricately involved when this ever happens, we need to take a look at their budgets.

I think the question is quite appropriate. Did the agency ask for more money?

The Social Security number, though, Mr. Chairman, is not confined to the issue of Medicare, whether it is on our Medicare cards. Social Security number is a problem across the board for most Americans. Let's address it. We don't want to address it. We only want to address it in the areas that are appropriately political. But the average American goes through a tremendous amount of nonsense, whether it is through their credit card, whether they are going for credit in a store, about giving up their Social Security number. And I think we need to take a look at that. Because no one on this side of the dais up here at the dais would admit or agree, rather, that this is confined to simply those people primarily over 65 years of age.

We have a very serious Social Security number problem, and we are not addressing it, Mr. Chairman. And we don't address it at our own peril. Wouldn't you agree? And we need to do something about that. Because the American people are very frustrated, the average American, if you ask them about this. You know, "What's your Social Security number?" Whatever we do nowadays. They will be asking for our Social Security numbers when we walk into theaters soon. Don't—you know, don't be surprised. Because go back 25 years and see how much more intrusive that has become in America.

I am very concerned about that, very concerned. I think it is just as big a problem as cyber security is on a national security level. And if we don't address it, it only brings the average citizen to have less faith in their government. And having someone over your shoulder.

And, by the way, most of these numbers are not used in the final analysis to take money from people fraudulently. It is used by commercial interests. They sell these numbers. Isn't that interesting? Why aren't we up here talking about that? Well, it is not our issue here. But the point of the matter is I think that is a bigger concern to us on a day-to-day basis. You would be shocked to know where your Social Security winds up—your number winds up, rather.

So, on an issue that we may debate as to whether we should privatize it or demonize it or eradicate it all together, that number becomes very valuable to commercial interests. Wouldn't you say, Mr. Trenkle?

Mr. TRENKLE. Yes, I would agree. It is certainly used in a number of areas. I know with my aunt, as I mentioned, closing out her estate, until we had the Social Security number none of the banks would even work with us to work on closing out the estate.

Mr. PASCARELL. What—how long do you think these changes are going to take, the ones that have been recognized today, eight years ago, five years ago? How long is it going to take? Mr. Bertoni or Mr. Trenkle, how long will it take to implement these specific changes? Whether you are going the first method, the second method, or the third option?

Mr. TRENKLE. Well, we estimated in the latest cost estimate that it would take four years: three years for planning, and then a year to issue the new numbers to each of our beneficiaries.

Mr. PASCARELL. Well, you are talking about issuing new cards as well, correct?

Mr. TRENKLE. That is correct. It would require new cards, as well.

Mr. PASCARELL. And would the cards necessarily have new numbers on them?

Mr. TRENKLE. If we moved to a new identifier, yes, they would have the new identifier.

Mr. PASCARELL. Might those numbers be hidden from the general public or anyone else, rather than simply pronounced on the card?

Mr. TRENKLE. That is one option.

Mr. PASCARELL. I don't see that option here.

Mr. TRENKLE. That is correct.

Mr. PASCARELL. So the issue about—and I will end on this point, Mr. Chairman—the issue about, you know, where are we really in this cost estimate and trying to get something done at the request of the Congress of the United States is a very serious question. The folks on both sides of this aisle have asked that question. And I don't think you come up with a pretty solid answer.

And I don't mean this as a criticism so much as you appreciate the frustration, but we are talking about pretty serious stuff here. And I would think that your association need not get back to us two years from now, but it needs to get back to us, your agency, pretty quickly.

Mr. TRENKLE. I certainly take it seriously. As you know, the 2006 estimate was done under the previous administration.

Mr. PASCARELL. Right.

Mr. TRENKLE. The 2011 one was done under this administration.

Mr. PASCARELL. Right.

Mr. TRENKLE. And I understand there is bipartisan support for doing that. And as I have said, I have committed today to going back and re-doing the estimate, getting it to you within the six months, with the possible caveat about Medicaid, and working with the committee and others to reprioritize if we don't get additional appropriations to work with you towards a solution on this.

Mr. PASCARELL. Mr. Chairman.

Chairman JOHNSON. Thank you.

Mr. PASCARELL. Would it be too much to ask before we leave our general meetings this year, that we get a report in September—

Chairman JOHNSON. Well, I was going to suggest why does it take six months for an estimate, let's try one month. Can you?

Mr. TRENKLE. Well, here is—I—we can certainly give you an estimate within a month. But as several of you members have said, and as the GAO said, they had concerns about how we did the analysis. So, in order to do an analysis correctly, I think we need to go back and look at how it was done, apply more of the rigor that GAO has suggested, and come forward to you.

There may be parts of this analysis we can get to you sooner than six months. But what I am just saying is I want to go back and do this in a way that satisfies our colleagues from GAO and satisfies all of you that we have done the rigor that you feel is necessary.

Chairman JOHNSON. Okay, thank you. The gentleman's time has expired. Mr. Smith, you are recognized.

Mr. SMITH. Thank you, Mr. Chairman. Mr. Trenkle, if we could perhaps reflect a little bit on the fact, I believe, that the Railroad Retirement Board uses non-Social Security beneficiary numbers for some of its members. Is that accurate?

Mr. TRENKLE. Yes, that is correct.

Mr. SMITH. And can you reflect a bit on how that can be, and yet it seems to be such a heavy lift for the rest of CMS to use similar software and other means to accomplish moving beyond the Social Security number identity?

Mr. TRENKLE. I can't speak for the Railroad Retirement Board. I know, in terms of scalability, the Railroad Retirement Board retirees are a small fraction of the number of Medicare beneficiaries. I believe they are in the hundreds of thousands, as opposed to 50 million.

Mr. SMITH. Okay. So if the GAO folks would reflect on that, perhaps, do you have any input?

Ms. KING. Yes. I think there are about 550,000 Railroad Retirement beneficiaries, so a much larger number. And I think probably one of the key differences is that the Medicare number is used by every provider for billing. And those billing systems are—some of them are legacy systems, some of them are antiquated, and it is a very complex network. And when you are changing the number,

you have to change it throughout the system. So, I think that is where a lot of the complexity comes in.

Mr. SMITH. But the software and the infrastructure to carry that out is already existent. Is it not?

Ms. KING. I can't quite answer that, because I don't know exactly what the Railroad Retirement Board is doing.

Mr. SMITH. Mr. TRENKLE.

Ms. KING. But I think they are one system, compared to—CMS has almost 50.

Mr. TRENKLE. Yes, they have a much smaller IT infrastructure, and we are talking about many more systems within CMS. And much of the Railroad Retirement Board IT work is supported by SSA a lot more closely than what it is with CMS. And, of course, you know with CMS we have quality areas that we support. We have the program integrity and a number of other areas that impact the use of the number throughout our various systems.

Mr. SMITH. And I don't want to over-simplify the issue, but it would seem to me that if it is possible to have a fairly—I mean smaller number, but still sizeable, to implement that conversion, I would hope that it could be done on a larger scale.

And on that similar issue, though, it looks like the CMS report suggests that it would cost roughly \$68 million to replace the 47 million cards at about \$1.44 per card. Is that accurate?

Mr. TRENKLE. Yes, that is accurate.

Mr. SMITH. Okay. And a little research would show that some private insurance companies did voluntarily remove the numbers, Social Security numbers, from their beneficiary cards over the last 10 years. And research shows that that costs about \$.70 to \$1, including shipping and handling. Can you elaborate on the difference between those costs?

Mr. TRENKLE. No, I can't. I would have to look at the assumptions used to derive their costs, as opposed to deriving our cost. So I can't comment on that here.

Mr. SMITH. Okay. I would be interested to know more, actually, in terms of how there could be such a difference between those numbers.

Thank you. I yield back.

Chairman JOHNSON. Thank you. Mr. Blumenauer, you are recognized.

Mr. BLUMENAUER. Thank you, Mr. Chairman, and I appreciate Mr. Smith's admonition he didn't want to over-simplify it. And I think that is important.

Is there any comparable system, in terms of number of participants, number of individual vendors, and scale, that would be—could—that you can return to that is anything like what you are being asked to do?

Mr. TRENKLE. Not in—well, certainly not in terms of scale and the tie-ins with the other major benefit programs that we have.

Mr. BLUMENAUER. Well, I mean, I think this is—I mean I want us to pursue progress in this. But I—one of the things that concerns me when people are talking about \$.70 to print a card, or \$1.50 to print a card, we are talking about over 52 million senior citizens. And millions—or not millions, but over a million small

businesses, some of whom are—you know, we are trying to nudge into the world of electronic records keeping.

It has taken the Federal Government a long time just to get to the point where Veterans and the Department of Defense have systems that can talk to each other. And those are, you know, pretty self-contained, part of the same family.

And I do think we ought to pause for a moment and think about the scale of what is being asked. Not that we shouldn't have more progress, not that I excuse what Mr. Doggett pointed out in terms of foot-dragging in the Bush Administration or failure in the Obama Administration to make progress, but there is a lot on the table. And this isn't an insurance company reprinting cards. This—I can just imagine the outrage that we would have in hearings if, all of a sudden, 52 million voting senior citizens get something that was screwed up.

So, I want to talk just for a second about—where are you in the organization? You are not the director. Is there anybody between you and the top?

Mr. TRENKLE. Yes, yes. I am a career—

Mr. BLUMENAUER. A career professional.

Mr. TRENKLE. Yes, correct.

Mr. BLUMENAUER. You care about your job, you show up?

Mr. TRENKLE. Absolutely.

Mr. BLUMENAUER. I wanted to just make sure that you had a chance to say that.

But do people in your position throughout the Federal Government freelance and interpret congressional priorities or budget priorities to put in—insist upon things that are going to be in your budget, or do you respond to priorities from OMB and from the administrator of the agency?

Mr. TRENKLE. It is the latter, yes. We respond to that.

Mr. BLUMENAUER. Okay.

Mr. TRENKLE. As, of course, obviously, a congressional—

Mr. BLUMENAUER. And if we had hundreds of people like you throughout the Federal Government who thought that this was a good idea, or thought that the Federal Government should do this, or that Congress was saying that, we would have kind of a chaotic budget process, wouldn't we?

Mr. TRENKLE. Yes.

Mr. BLUMENAUER. Have you ever experienced Congress speaking with different words and having different priorities, and asking one thing and not funding it as a priority? Have you ever seen that in your public service career?

Mr. TRENKLE. Yes, I have.

Mr. BLUMENAUER. Mr. Chairman, I think we ought to cut slack for career civil servants who are doing their job. And I resent somehow an implication that people who are doing their job and following priorities that have been in Republican and Democratic administrations, somehow they don't care, that somehow, because they haven't arrested somebody for identity theft, that they are not aware of it and concerned about it. I just am concerned about the tone and nature of this.

Because I think we ought to make progress. I think that it is hopeless—it is very complex. I have had, in a prior life, a little experience with personnel systems and data processing. And so I am not excusing what prior administrations have not done, or what prior congresses have not done to stay on top of it and fund it. But I would just hope that we are a little more respectful for the men and women who are professionals, doing their job, and trying to follow what they are told to do, not freelancing. And I think we would have people here outraged if folks were freelancing interpreting what the Congress did.

We have got a little legislation, Mr. Gerlach and I—who is a little agitated, and I appreciate that—but we have legislation that would establish a pilot project, H.R. 2925, that would have a secure piece of identification, to see if we could have something that would enable a better way of paying, a better way of securing identity, getting numbers off, making it individual so that CMS and others could track compliance, but would be easy for providers.

Is there some way that we could explore something along this line, as a constructive alternative to meet both these objectives?

Mr. TRENKLE. I am assuming you are talking about the use of smart cards, or—

Mr. BLUMENAUER. Yes, sir.

Mr. TRENKLE [continuing]. Or other types of technology.

Mr. BLUMENAUER. Yes, sir.

Mr. TRENKLE. I certainly think that is something worth looking into. I think that I have had a fair amount of experience working with smart cards over the last 15 years, and I know there are some issues around scalability, particularly as you can think about the number of cards that we have to replace on a monthly basis.

Mr. BLUMENAUER. Right.

Mr. TRENKLE. Also, the number of providers we have to deal with who would have to get readers. But I certainly think it does offer some possibilities, it and other technologies.

Mr. BLUMENAUER. I see my time has expired, Mr. Chairman. But I would just put that on the table, that Mr. Gerlach and I have legislation that would have a pilot project to be able to answer some of these questions, to test it, that might be easier for 52 million senior citizens, and get at that big fraud number in a way that isn't just reprinting cards, but really gets at the system.

Chairman JOHNSON. Okay, thank you.

Mr. BLUMENAUER. Thank you. I appreciate your courtesy.

Chairman JOHNSON. Thank you for your comments. Mr. Bertoni, decades ago we co-opted the Social Security number, using it for all kinds of non-Social Security purposes. And recently, both the private and the public sector are moving away from these numbers. What can you tell me about this trend, and why has it occurred? And what are some of the entities that have reduced or eliminated their use or display of Social Security numbers?

Mr. Bertoni. Actually, in preparing for this, I went through a number of our prior GAO reports, and actually have a long list of folks who have made progress.

I think that the issue of use and display, first of all, we have come to where we are because, as some of you have said today, using the SSN is easy. It is convenient. It is tied to so many life

transactions, it is a way for both public and private sector entities to determine who you are, and especially the private sector, to determine whether they want to do business with you.

So, from a use standpoint, I think both public and private sector, the SSN continues to be pervasive. And I don't believe there has been much progress in there. We have the OMB memorandum, of course, we had some other initiatives. But I still think the use of the SSN is as pervasive as it was several years ago.

But when you get to the area of display, I do believe there has been a lot of progress. I think that is the easy part. People realize that we can't have these SSNs emblazoned on documents, on cards. And there has been a movement over the last decade or so to remove them.

Now, starting with the higher education, we no longer have SSNs on student IDs. Easy to do. The 50 states, when—at one time the SSN was on every driver's license, per the direction of the Congress. The states have now redacted all of those. We have had state and local governments who are—many of which are engaging in pretty aggressive initiatives to remove Social Security numbers from state and local public records. And certainly we have the large federal agencies like DoD and VA getting out on this issue. And lastly, the private insurance companies, getting SSNs off the cards.

I do believe I will say that a major outlier is CMS. They are behind the curve on this with 48 million cards on the street. I think it is time that they have caught up with the rest of the world and started moving to an environment where the SSN is not on the card. Most people don't know how their identity was stolen. Sixty-five percent of people don't know how that happened, or who did it. But in the 35 percent of the population of the victims that know it the second most frequent source of identity theft is a stolen wallet, a stolen purse, or interception in the mail. And you are going to find Medicare cards in all three of those places.

Chairman JOHNSON. Thank you. I appreciate that comment.

Mr. Becerra, do you have a closing comment?

Mr. BECERRA. I do, Mr. Chairman. And it is inspired by some of the things that Mr. Bertoni just said, as well.

Mr. Trenkle, I think, as you noticed, there is complete bipartisan agreement that we have got to get the number off of the card. And there may be a bit of a breakdown, as I think Mr. Blumenauer tried to point out, about how we get there. But I don't think there is any doubt that, at least in this House—and I got to believe our colleagues in the Senate would agree—that it really is time, as Mr. Bertoni said, for CMS to catch up and remove the number from the card.

But, Mr. Chairman, let me suggest something to those of us who have taken an interest in this issue here in Congress. I agree with you that I think the re-estimate shouldn't take six months. You have done some work, both in 2004/2005 and 2010/2011 to come up with that estimate. You don't have to re-invent the wheel to come up with an estimate.

But let me suggest as well that if we work closely with GAO—and, Mr. Chairman, I think you are as interested in this as any, as Mr. Doggett and others have proven by authoring legislation—if we take it upon ourselves to bird dog this with CMS so that CMS

understands how critical we think this is, and that we can have some bipartisan consensus about how to get this done, including dealing with the resources issue, then maybe what we can do is accelerate their time frame to get us an estimate, having participated with them in the process of coming up with this estimate, working with GAO and others who could do the non-partisan oversight.

Maybe what we can do is, when they issue their finding about what it would cost, we are prepared to act because we will have been monitoring this all the way through, versus going through a process of holding hearings and have a hearing or a conversation or a disagreement about what it would take to get there.

And my sense is that there is no lack of enthusiasm on the part of Democrats or Republicans to get this done. It is going to be more an issue of how we actually implement whatever a reasonable estimate says we should do. And so I would hope that maybe what we can do is—to show our bonafides on this side of the dais—is keep tabs of CMS in a friendly way, but keep tabs and ride herd on you. And hopefully, with GAO's participation, come up with those answers that we still don't have: the resources, how quickly can you reprioritize, how much will you need in new additional resources, what will be the impact on current activities.

And if we can do that, Mr. Chairman, I think we can save ourselves a lot of problems and bickering about how to actually get it done, and do it a lot faster than if we just allowed the bureaucracy to move this forward.

So, I just offer that in the spirit of bipartisanship, to try to get this done, and also to let CMS know that we hope that they are hearing this clearly, that this is something that we want to really monitor with them.

Yield back.

Chairman JOHNSON. Thank you. I appreciate your comments. And I thank you all for your participation today. It is a joint effort. It is not one party or the other.

Thank you all for being here today and for your testimony. I look forward to continuing working with my colleagues to protect seniors from identity theft.

With that, this joint hearing stands adjourned.

[Whereupon, at 11:14 a.m., the subcommittee was adjourned.]

Member Questions For The Records

Tony Trenkle

Tony Trenkle's Additional Written Questions
For the Record
"Removing SSN's from Medicare Cards"
House Ways & Means Social Security & Health Subcommittees

August 1, 2012

From Chairman Sam Johnson & Chairman Wally Herger

Questions for the Witness

- 1. At the hearing, you indicated you have consulted with the Defense Department and the Department of Veterans Affairs about how they developed a strategy for removing the SSN from their ID and medical cards. Please describe the specific results of these consultations.**

Answer: CMS discussions on this issue with the Department of Defense and the Department of Veterans Affairs lead us to believe that a transition away from the Social Security Number as Medicare ID would be much more challenging for CMS than it was for DOD and VA. In particular, the size and scope of the Medicare program is many times larger than DOD and the VA. The VA provides health care coverage to approximately 8.6 million veterans and their families, while the DOD provides health care to 9.6 million beneficiaries. In contrast, Medicare annually processes about 1.3 billion claims from about 1.5 million providers on behalf of more than 50 million Medicare beneficiaries. These differences in size and scope make it more technically challenging and costly to implement a lengthy, phased transition as DOD and the VA conducted because of the necessity of operating two parallel systems of identification during the transition. In addition the ability of DOD and the VA to continue to embed the SSN electronically in ID cards during the transition is not an option available with the current paper Medicare card.

- 2. In their testimony, the Government Accountability Office (GAO) stated that, of the three options for removing SSNs from Medicare cards that were presented in CMS's 2011 report, replacing the SSN with a new identifier for use by beneficiaries and providers would offer the greatest protection against identity theft. Does CMS agree with GAO's assessment of the three options regarding the risks and vulnerabilities associated with the need to protect beneficiaries' data?**

Answer: CMS agrees that such an approach could protect beneficiaries from identity theft from loss or theft of the card itself. Additionally, as our November 2011 report explained, replacing the SSN with a new identifier would allow CMS to "turn off" a beneficiary number that had been compromised, which could prove a useful tool in combating Medicare fraud and medical identity theft. CMS agrees that of the three options presented in the 2011 report, this option would best

meet the goals of reducing the risk of identity theft and preventing fraud while minimizing the burden on beneficiaries and providers.

3. What other solutions, besides the three presented in the 2011 assessment, were considered by CMS as options for removing the SSN from Medicare cards? To what extent did CMS examine other approaches currently in use by private insurers, financial institutions, and other government-run health care entities?

Answer: CMS considered providing a new, non-SSN-based identifier to newly-enrolled beneficiaries and maintaining the current SSN-based HICN for existing beneficiaries, but concluded it would be cost-prohibitive to maintain parallel systems of beneficiary identification for an extended period of time and that there would be no benefits for current beneficiaries in identity-theft mitigation or fraud prevention. CMS interviewed members of the information technology departments of private insurers to learn about the systems and beneficiary and provider outreach challenges they faced when transitioning to a new identifier.

4. In any of the three options, did CMS consider the implementation of mechanisms that could eliminate the need for CMS to modify each of the affected CMS systems? For example, did CMS consider any solutions that would translate new identifiers to SSNs at a single point of entry, rather than require modifications to each system to accept new identifiers? Were the effects on the time and costs of implementing any such approaches considered when CMS developed cost and schedule estimates?

Answer: All of the three options assumed that affected systems would use a translation mechanism rather than a complete internal replacement of the Health Insurance Claim Number (HICN) with the Medicare Beneficiary Identifier (MBI). Even a translation alternative would require changes for all affected systems. It is not possible to make these changes at a “single point of entry” because CMS systems have numerous external points of communication, with data coming in and going out. Each of those systems would require modification in order to use the translation mechanism. As CMS revisits its cost estimates, we are endeavoring to define with more precision the extent and costs for the required modification of every system and the extent to which the use of a translation mechanism could minimize those modifications and costs.

5. Were alternative analyses conducted for each of the solutions presented in the 2011 assessment and/or for any other options? Please provide supporting documentation, if any, that show the results of these analyses.

Answer: No, CMS developed a rough order of magnitude cost estimate for the systems changes and outreach and education associated with each option. CMS is currently in the process of revising these estimates to provide greater precision as to the implementation costs.

a. To what extent were detailed technology assessments conducted to determine the impact on existing CMS, Railroad Retirement Board (RRB), the Social Security Administration, and other external entities’ systems?

Answer: In conducting the 2011 assessment of the costs associated with different options for removing the SSN from the Medicare beneficiary card, CMS looked at the impact of changing the beneficiary identifier on Medicare on existing CMS systems that would be affected and provided a rough order of magnitude estimate of the costs of those impacts. Because it was beyond the scope of the Congressional request and because there are additional cost and policy considerations tied to the adoption of new technologies, CMS did not analyze these options or estimate their costs in the context of the possible adoption of new technological solutions for beneficiary identification, such as “smart cards” or a global revamping of CMS legacy systems.

- b. Were any entities independent of CMS, such as technology consultants, involved in conducting any such assessments? If so, please identify. If not, please explain the reasons why.**

Answer: We did not have independent technology consultants conduct third party feasibility or development assessments because it was beyond the scope of the Congressional request.

- c. Please provide reports of any technology assessments that were conducted by CMS and any other entities involved.**

Answer: CMS did not conduct a technology assessment, nor did any other entity.

- 6. As noted in the 2006 assessment, CMS systems already map multiple identifiers for beneficiaries to the identifiers printed on Medicare cards. Also, RRB identification numbers are maintained and processed by CMS’s and others’ systems.**

- a. How are these identification numbers processed by CMS’s information systems? Are they “mapped” or otherwise translated to SSN-based identifiers, or are they stored, maintained, and processed differently than the SSN-based identifiers?**

Answer: The multiple identifiers for beneficiaries mentioned in the 2006 assessment referred to CMS systems maintaining a history of the beneficiary Health Insurance Claim Number (HICN) and RRB numbers. The 2006 assessment was not referring to a different beneficiary identifier other than the SSN-based one that SSA and RRB send to CMS. The RRB sends CMS RRB numbers as opposed to HICNs. The HICN can change during a beneficiary’s lifetime; as a result, CMS systems keep a table in their databases that links the most current HICN/RRB number to prior valid HICNs/RRB numbers for the beneficiary.

- b. What implications to the cost of implementation and maintenance of the systems would this approach introduce if used in efforts to remove the SSN-based identifier from Medicare beneficiaries’ cards?**

Answer: In order to interface with SSA and other Federal agencies, CMS still needs to maintain the RRB number that is provided by RRB and the combination of SSN and identification code which is provided by SSA that CMS uses as the HICN. As a result, CMS cannot simply reuse the existing data element and replace it with the new beneficiary identifier. The new beneficiary

identifier would need to be stored separately from the HICN/RRB number. The new beneficiary identifier would add more data, including history of the new identifier when it changes, a crosswalk of the new identifier to the HICN/RRB number, as well as the ability to retrieve the new identifier.

Kathleen King



September 21, 2012

The Honorable Sam Johnson, Chairman
Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

The Honorable Wally Herger, Chairman
Subcommittee on Health
Committee on Ways and Means
House of Representatives

The enclosed information responds to the posthearing questions in your letter of September 7, 2012, concerning our testimony before your committees on August 1, 2012, on removing Social Security numbers (SSN) from Medicare cards. If you have any questions or would like to discuss this information, please contact us at (202) 512-7215, or (202) 512-7114, respectively.

Sincerely yours,

A handwritten signature in cursive script that reads 'Dan Bertoni'.

Dan Bertoni, Director
Education, Workforce, and
Income Security Issues

A handwritten signature in cursive script that reads 'Kathleen M. King'.

Kathleen M. King, Director
Health Care Issues

Enclosure

Enclosure

The enclosure provides your questions and our responses for the record and supplements information provided to your committees in our testimony, *Action Needed to Remove Social Security Numbers from Medicare Cards* (GAO-12-949T, Washington, D.C.: Aug. 1, 2012).

Questions for the Record

The Honorable Sam Johnson, Chairman
Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

The Honorable Wally Herger, Chairman
Subcommittee on Health
Committee on Ways and Means
House of Representatives

1. To your knowledge, is it common for Federal agencies to submit final reports to Congress without following proper standards of data documentation?

We have not conducted the work necessary to answer this question.

2. Is the CMS report a document that Congress should use to make policy decisions, or is it too unreliable to be the basis for any reasonable policy decision?

In our view, the 2011 report to Congress is not sufficient for making policy decisions if Congress considers cost a factor in such decisions. First, the Centers for Medicare and Medicaid Services (CMS) did not use any cost estimating guidance when developing the cost estimates presented in this 2011 report to Congress. Second, the procedures CMS used to develop estimates for the two largest cost categories—changes to existing state Medicaid information technology (IT) systems and CMS's IT system conversions—are questionable and not well documented. Third, there are inconsistencies in some assumptions used by CMS and the Social Security Administration, such as the number of beneficiaries, to develop estimates. Finally, CMS did not take into account other factors when developing its cost estimates, including related IT modernization efforts or potential savings from removing the SSN from Medicare cards.

3. Based on your extensive body of work on identity theft and SSN integrity, can you help us understand what role the SSN plays in facilitating identity theft? How would someone be able to commit identity theft after obtaining an SSN?

Although the SSN was originally created as a means to track workers' wages and Social Security benefits, because of its unique nature and broad applicability, it has become the identifier of choice for public and private sector entities and is used for many non Social Security purposes. Today the SSN, sometimes along with other documents, is often required as proof of identity to apply for or receive government benefits, obtain credit, and open a bank account, among other things. The SSN is generally needed to obtain key identity documents such as drivers' licenses. As a result, an SSN is highly valuable to identity thieves and can act as a "breeder" document. Once in possession of an SSN, along with other personal data such as name and date of birth, criminals can obtain identity documents and thereby assume those identities. This facilitates their ability to commit financial or other crimes undetected.

4. Would you please summarize the reasoning behind your belief that the approach you selected in your testimony—replacing the SSN with a new Medicare identification number that is also used by beneficiaries and providers—is the best of the three CMS-identified options?

As we noted in our report, our analysis focused on the options presented by CMS rather than an assessment of all potential options that might exist. Of the options presented by CMS, the option that calls for developing a new identifier for use by beneficiaries and providers offers the best protection against identity theft and presents fewer burdens for beneficiaries and providers than the other two options presented in CMS's 2011 report to Congress. Under this option, only the new identifier would be used by beneficiaries and providers. This option would lessen beneficiaries' risk of identity theft in the event that their Medicare card was lost or stolen, as the SSN would no longer be printed on the card. Additionally, because providers would not need to collect a beneficiary's SSN or maintain that information in their files, beneficiaries' vulnerability to identity theft would be reduced in the event of a provider data breach. The other two options provide less protection against identity theft because providers would still need to collect the SSN, leaving beneficiaries vulnerable to identity theft in the event of a provider data breach. Finally, the option that involves replacing the SSN with a new identifier for both beneficiary and provider use presents the fewest burdens for beneficiaries and providers relative to the other two options presented in CMS's report to Congress. Under this option, the new identifier would be printed on the card, and beneficiaries would use this identifier when interacting with CMS, eliminating the need for beneficiaries to memorize their SSN or store it elsewhere as they might do under the other options. This option may also present fewer burdens for providers, as they would not have to query databases or make phone calls to obtain a beneficiary's SSN in order to submit claims. In our report, we recommended that CMS select an approach for removing SSNs from Medicare cards that best protects beneficiaries against identity theft and minimizes burdens for providers, beneficiaries, and CMS.



Public Submissions For The Record

AARP



August 1, 2012

The Honorable Sam Johnson
Chairman
Subcommittee on Social Security
House Ways & Means Committee
Washington, DC 20515

The Honorable Wally Herger
Chairman
Subcommittee on Health
House Ways & Means Committee
Washington, DC 20515

Dear Representatives Johnson and Herger:

On behalf of the millions of AARP members, and the millions more who rely on Medicare, thank you for holding a hearing to examine protecting Medicare beneficiaries' identities, and reduce fraud, by removing Social Security numbers (SSN) from Medicare cards. Many of our members are victims of identity theft, and many older Americans express concerns about the risks of having a Medicare card go missing.

The Federal Trade Commission estimates that as many as 10 million Americans have their identity stolen each year. Unfortunately, the 48 million Medicare beneficiaries have no choice but to have their SSN displayed on their Medicare cards. Because both government agencies and private businesses use SSN for a wide range of non-Social Security purposes, having your SSN fall into the wrong hands exposes your most important personal information to identity theft. Most Medicare beneficiaries carry their card with them, which leaves them vulnerable to identity theft if their wallets or purses are lost or stolen. While we urge all Medicare beneficiaries to treat their Medicare cards with the same prudence as they would their credit cards, and guard them safely, a lost SSN is not easily replaced.

Moreover, having a SSN on a Medicare card makes it easier to commit fraudulent billing. Criminals can set up false patient accounts using real beneficiary names and information. Fraud and abuse cost the Medicare program billions of dollars each year. Small changes, such as removing Social Security numbers from Medicare cards, can help improve program integrity.

There are several legislative proposals introduced in Congress that would help reduce waste, fraud, and abuse in Medicare. In addition to Chairman Johnson's *Medicare Identity Theft Protection Act*, these bills also promote safer, more secure programs by addressing beneficiary identity theft.

S. 1551/H.R. 2925 – The Medicare Common Access Card Act of 2011

This bill would establish a pilot program in order to utilize smart card technology for Medicare beneficiary and provider identification cards. The smart cards would provide greater security for beneficiaries' personal information, thereby reducing the possibility for identity theft. The technology would also enable more responsive claims tracking and adjudication, as well as reduce provider administrative burden.

H.R. 978 – The Seniors' Identity Protection Act of 2011

This bill would remove Social Security numbers from certain government-issued cards used in connection with Medicare, Medicaid, and CHIP programs.

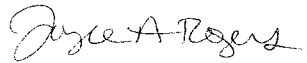
S. 1251/H.R. 3399 – The Medicare and Medicaid Fighting Fraud and Abuse to Save Taxpayers' Dollars Act (otherwise known as the Medicare and Medicaid FAST Act)

This bill would prohibit the display of Social Security numbers on newly issued Medicare identification cards. Moreover, this legislation would strengthen many existing programs by improving data sharing across federal agencies and programs in a way that would ensure more real-time sharing to discourage and prevent payment of fraudulent or duplicate claims. The legislation would also include additional penalties for people who illegally distribute Medicare, Medicaid, or

CHIP beneficiary identification information or provider billing privileges, and improve upon the Senior Medicare Patrol (SMP), which helps educate beneficiaries to detect and report Medicare waste, fraud, and abuse.

The Medicare program must be worthy of beneficiaries' trust, particularly when using sensitive personal information. By removing visible SSN from Medicare cards, we can reduce the likelihood of identity theft and fraud. AARP looks forward to working with the Committee as you address this important issue. If you have any questions, please feel free to contact Ariel Gonzalez of our Government Affairs staff at 202-434-3770 or agonzalez@aarp.org.

Sincerely,



Joyce A. Rogers
Senior Vice President
Government Affairs



Kenneth Ryesky

Kenneth H. Ryesky SSNs on Medicare Cards: 5 August 2012 Page 1

**KENNETH H. RYESKY, ESQ., STATEMENT FOR THE RECORD, UNITED STATES
HOUSE OF REPRESENTATIVES COMMITTEE WAYS & MEANS,
SUBCOMMITTEES ON SOCIAL SECURITY AND ON HEALTH, JOINT HEARING
ON SOCIAL SECURITY NUMBERS ON MEDICARE CARDS:****I. INTRODUCTION:**

The House Ways & Means Committee, Subcommittees on Social Security and on Health held a Hearing on 1 August 2012, regarding the use of Social Security Numbers (SSNs) on Medicare Cards. Public comments were solicited. This Commentary is accordingly submitted.

II. COMMENTATOR'S BACKGROUND & CONTACT INFORMATION:

Background: The Commentator, Kenneth H. Ryesky, Esq., is a member of the Bars of New York, New Jersey and Pennsylvania, and is an Adjunct Assistant Professor, Department of Accounting and Information Systems, Queens College of the City University of New York, where he teaches Business Law courses and Taxation courses. Prior to entering into the private practice of law, Mr. Ryesky served as an Attorney with the Internal Revenue Service ("IRS"), Manhattan District. As detailed below, he has submitted commentary for recent Congressional hearings on related matters.

Contact Information: Kenneth H. Ryesky, Esq., Department of Accounting & Information Systems, 215 Powdermaker Hall, Queens College CUNY, 65-30 Kissena Boulevard Flushing, NY 11367. Telephone 718/997-5070; E-mail: khresq@sprintmail.com.

Disclaimer: This Commentary reflects the Commentator's personal views, is not written or submitted on behalf of any other person or entity, and does not necessarily represent the official position of any person, entity, organization or institution with which the Commentator is or has been associated, employed or retained.

III. COMMENTARY ON THE ISSUES:**A. Previous Hearings:**

The instant proceeding of 1 August 2012 is not the first to deal with the uses of SSNs. Ways and Means hearings were held on 2 February 2012 and 8 May 2012, and the Fiscal Responsibility & Economic Growth Subcommittee of the Senate Finance Committee also held

hearings on 25 May 2011 and on 20 March 2012. The Commentator submitted Statements for the Record for the hearings of 2 February 2012,¹ 20 March 2012² and 8 May 2012.³ 2012 TNT 95-49

The aforementioned prior commentaries addressed the uses, misuses and abuses of the SSNs of deceased individuals in connection with tax fraud. The instant Hearing, hence this instant Commentary, primarily addresses the uses, misuses and abuses of the SSNs of living individuals. The two implicate differing dynamics, and warrant differing countermeasures.

B. The Ubiquity of SSNs:

Over the years, the SSN's use has expanded from an identifying number for participation in the Social Security program to the very identity of the SSN holder. During the 1970's, when the Commentator was a college undergraduate, the standard practice was to use the SSN as the student's identification number, which was embossed upon the student identification cards issued by the colleges. When the Commentator applied for gainful part-time employment, the prospective employer did not accept the applicants' word as to what their SSN was, but insisted upon something "official." The Commentator's college identification card was readily accepted as an "official" indicium of his SSN.

In short, what once were common, accepted and sensible uses of the SSN are now dangerous and, ever increasingly, have become forbidden. Many organizations have had to undergo culture changes in the shift away from SSNs.

C. The Commentator's Personal Experience: An Innocent Inadvertent Breach:

In connection with what proved to be the final illness of the Commentator's father, the nursing home sent a bill which had an attached print-out from the local Blue Shield affiliate. The print-out form listed five patients at the facility, each with the Medicare number (which was one and the same as the SSN). The line for the Commentator's father was highlighted. Presumably, the other four patients or their families were sent bills with the same attachment, the name of each respective corresponding patient having been marked with a highlighter marker

¹ Posted on the internet at <<http://www.fgs.org/rpac/wp-content/uploads/2012/02/wm-ssdmf-comments-2012.pdf>>, also available at 2012 TNT 25-32.

² Posted on the internet at <<http://www.fgs.org/rpac/wp-content/uploads/2012/04/senfincomm-taxfraud-20120320-corrected2.pdf>>, also available at 2012 TNT 56-30.

³ Posted on the internet at <<https://docs.google.com/open?id=0B0erD-E9YY0rOXAtamx1cmJYdjQ>>, also available at 2012 TNT 95-49.

The nursing home had thus disclosed the SSNs of each patient to one or more third parties having no need to know the SSN.

This particular incident appears to have been an honest and inadvertent mistake, and the Commentator is not aware that any negative consequences have befallen any of the patients involved. But one cannot ignore the potential for damage if such disclosure is done nefariously and intentionally.

Moreover, this incident demonstrates that removal of the SSNs from the individual Medicare cards would not be sufficient if the SSNs are used in other documents involved in the Medicare administrative processes.

D. The Example from Academia:

It is noted that many colleges and universities have successfully transitioned away from SSNs as student identification numbers.⁴ Such an action requires the issuance and use of substitute student identification numbers, and the promulgation and enforcement of rules regarding the use (and non-use) of SSNs by faculty, administration and other concerned parties. The Commentator was involved in the sweep of such an organizational culture change as a faculty member at the college where he teaches.

VI. CONCLUSION:

The respective testimonies of Ms. King and Mr. Trenkle each discuss the roadblocks to removing SSNs from Medicare cards, and each indicate that a concerted and coordinated effort must be undertaken in order to reach that goal.

While the Medicare system is far larger and far more complex than any individual college or university, it is likely that lessons can be learned from the experiences of the academic world, and applied towards the implementation of the goal to remove SSNs from Medicare cards.

Beyond the foregoing, the Commentator now takes this opportunity to remind the Subcommittee that Social Security Numbers were initially intended to be just that, identifiers for Social Security system participants;⁵ and dares suggest to the Subcommittee that Section 1211 of the Tax Reform Act of 1976⁶ [Pub. L. 94-455], while seemingly a sound legislative provision

⁴ Some states have legislatively mandated that such be done. *See, e.g.* N.Y. EDUC. L. § 2-b.

⁵ *See* Social Security Act of 1935, Pub. L. 74-271, § 807(b).

⁶ Pub. L. 94-455.

Kenneth H. Ryesky SSNs on Medicare Cards: 5 August 2012 Page 4

when enacted by their predecessors, has proven to be ill-advised and dysfunctional in its scheme to mandate the expansion of the functions of the SSN beyond its initial purpose.

5 August 2012
Respectfully submitted,

A handwritten signature in black ink, appearing to read "Kenneth H. Ryesky". The signature is written in a cursive style with some flourishes.

Kenneth H. Ryesky, Esq.



Secure ID Coalition

**Medicare Common Access Card:
Preventing Fraud Before It Happens**



**The Secure ID Coalition Report to the
Senate Committee on Finance
Medicare & Medicaid Program Integrity**

Kelli A. Emerick
Executive Director

June 29, 2012

TABLE OF CONTENTS

Improving Medicare & Medicaid Program Integrity	3
What is the problem?	4
What is the Solution?	5
How Medicare CAC Works in the Doctor's Office	7
How will Medicare CAC solve the problem?	8
What are the benefits of a Medicare smart card to beneficiaries, providers and taxpayers?	10
Where has this type of program been successful?	12
What are the costs of implementing Medicare CAC?	14
What is the return on investment and what is it based on?	15
Recommendations	16
Conclusion	17
Questions & Answers	17
Appendix	19
Additional Resources	19
Attached Documents	19

About the Secure ID Coalition:

Founded in 2005, the Secure ID Coalition works with industry experts, public policy officials, and federal and state agency personnel to promote identity policy solutions that enable both security and privacy protections. Because of our commitment to citizen privacy rights and protections we advocate for technology solutions that enable individuals to make decision about the use of their own personal information. Members of the Secure ID Coalition subscribe to principles that include the increased deployment of secure identity solutions, as well as advise on and advocate for strong consumer privacy protections and enhanced security to reduce waste, fraud, theft and abuse. Our mission is to promote the understanding and appropriate use of smart card technology to achieve enhanced security for ID management systems while maintaining user privacy. Such ID management systems include physical and/or logical access to facilities and networks. For more information, please visit our website at www.secureIDcoalition.org.

IMPROVING MEDICARE & MEDICAID PROGRAM INTEGRITY

Prevention is 90 Percent of the Cure

Our nation's Medicare and Medicaid programs are under attack. The combined cost of fraud, waste and abuse in both programs are estimated to reach over *\$100 billion a year* – and growing. The reason for such a monumental waste of taxpayer funds is a systemic lack of accountability: criminals posing as durable medical equipment providers billing Medicare for products never sold, rogue providers billing for services never rendered, and inattentive office staff billing Medicare for treatments never allowed. If fraud, waste and abuse within the Medicare and Medicaid systems are ever to be curbed, the very first place we need to start is being able to know and verify who is authorized to provide and receive these important benefits – while preventing those who are not – before the claim is ever made.

Unfortunately, our current inability to address this fundamental identity and verification problem leaves both the Medicare and Medicaid systems perpetually open to ongoing exploitation. Programs to curb Medicare and Medicaid fraud, waste and abuse without first resolving the identity verification problem will ultimately fail if we don't know who is a legitimate beneficiary or provider, and who is not.

Structuring the Medicare and Medicaid systems to prevent fraud will not only save taxpayers billions of dollars every year, but ensure that these two very important programs survive to serve Americans now and well into the future.

Securing the Cards and Transactions

This proposal addresses the problem of **identity verification** of beneficiaries, providers and suppliers as well as **securing billing transactions** in Medicare. The proposal calls for upgrading the Medicare card to secure transactions as has been done in other federal programs and other health programs across the world. Much of the content of this proposal is contained in the Medicare Common Access Card Act introduced last year in the both the House (HR.2925) and Senate (S.1551), both of which are endorsed by the American Association of Retired Persons (AARP). These bills call for an upgraded Medicare card, based on a secure smart card, to verify who is eligible to give and receive benefits as a pre-condition to the claim ever being presented to the Centers for Medicare and Medicaid Services (CMS) for payment.

Under the proposal for beneficiaries, the new smart card would securely store the Medicare account number or identifier (which today is the Social Security number) on a secure micro-controller. Providers and suppliers will also receive a new smart card, securely storing their National Provider Identity number (NPI), so that only they can use it. By requiring identity verification of providers and beneficiaries before a claim can be filed and payment processed, Medicare would easily eliminate more than fifty percent of the fraud within the current system.

Smart card solutions are used throughout the Federal government as employee credentials, within the States as benefits cards, and in local hospitals and health systems to reduce errors, eliminate duplicate electronic records and to save administrative costs. For the purposes of this paper, the program outlined calls out Medicare specifically. Our industry has been discussing and promoting an upgraded Medicare card to reduce fraud, waste and abuse within the program over the past several years.

However, smart cards could easily be deployed within Medicaid. Currently, several states including Georgia, North Carolina and Virginia are considering smart cards and biometrics programs as a way to reduce fraud, waste and abuse within Medicaid. The Secure ID Coalition continues to reach-out and dialogue with a number of healthcare providers and others in the healthcare community to educate them about the potential benefits of the smart card technology solution.

WHAT IS THE PROBLEM?

Provider-Based Fraud and Error:

- Phantom billing is where fraudsters or unscrupulous medical providers bill Medicare for unnecessary or unperformed procedures, medical tests, or equipment (or for equipment that is billed as new but is, in fact, used).
- NPI numbers of upstanding providers are stolen by fraudsters and criminals and used to file claims. In this case providers are unaware their Medicare account is being used for nefarious purposes.
- Durable medical equipment abuse can happen when medical equipment used in the home - like wheelchairs or oxygen tanks - are billed many times over, while in fact nothing has been delivered to an actual patient.
- Processing errors and mistakes account, in many cases, for improper payment. These payments either should not have been made or were made in an incorrect amount. Improper payments also include payments sent to the wrong recipient or payments where supporting documentation is not available.

Patient-Based Fraud:

- Fraudulent patient billing can occur when a patient provides his or her Medicare number to a provider in exchange for kickbacks. The provider bills Medicare for any reason and the patient is told to admit that he or she indeed received the medical treatment.

- “Card Swapping” passed-off or stolen Medicare cards are used by others to get medical care

WHAT IS THE SOLUTION?

A Medicare Common Access Card

The term “common access card” derives from the original federal government smart card program: The Department of Defense’s Common Access Card (CAC). The DOD CAC was implemented in 2000 as a means of authenticating personnel with access to DOD facilities and computers. Upon full deployment, network intrusions were reduced by nearly 50% overnight. The CAC model and platform has also been rolled out across the federal government for all employees and contractors known as the Personal Identity Verification (PIV) program.

A Medicare CAC would leverage the existing government platform for secure identity credentials to modernize how information is protected within the Medicare system itself. Doing so protects the personal information of every beneficiary and puts in place a front-end prevention system to only allow authorized providers and suppliers to bill for Medicare services.

Authenticating Medicare beneficiaries and providers during an enrollment process and requiring the use of secure personalized credentials will reduce fraud by:

- Verifying beneficiaries are authorized to receive services and pharmaceuticals or equipment being prescribed;
- Verifying providers are authorized to provide those services and bill Medicare;
- Verifying suppliers, such as durable medical equipment (DME) vendors, are authorized to provide products and/or services and bill Medicare
- Preventing imposters from posing as beneficiaries or providers, thereby thwarting fraudulent transactions; and
- Verifying and coding each transaction to prevent phantom billing, processing errors and DME abuse.

Further, an upgraded Medicare card would protect beneficiary’s privacy by taking their Social Security number off the front of the Medicare card, and locking it securely within the card’s onboard computer chip – an important step in helping to reign in identity theft.

Card Issuance and Use

Today when a beneficiary first enrolls in the Medicare program they verify their identity with documents or certificates on record with the Social Security Administration. Under Medicare CAC the process for beneficiary enrollment would not change. After electing to receive Medicare, beneficiaries receive a new secure smart card in the mail containing their protected

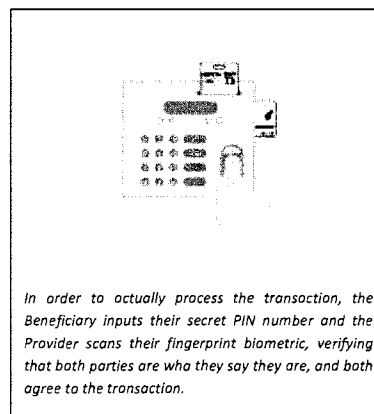
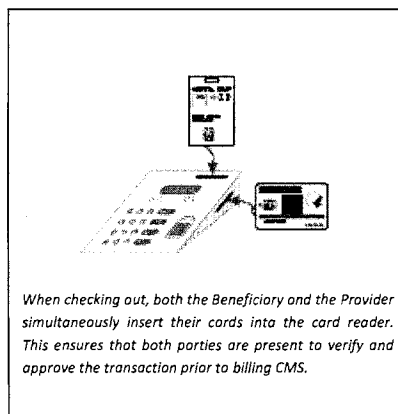
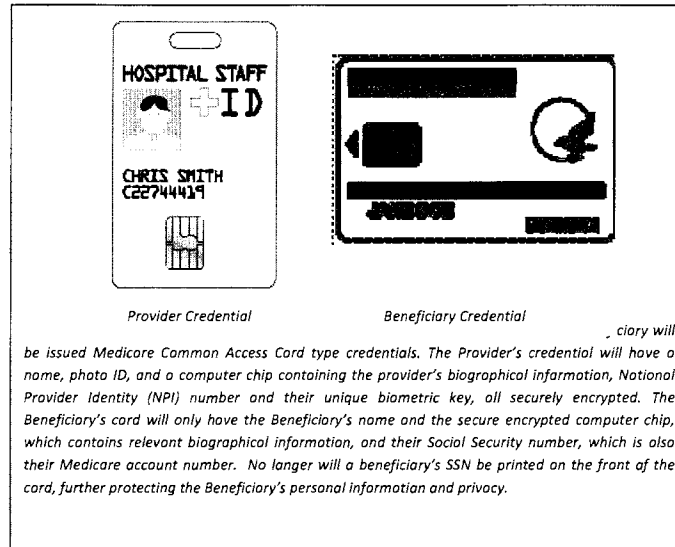
5

identification information on an embedded micro-controller. For security purposes, a unique PIN code would be mailed to the beneficiary separately. The card and PIN together authenticate the beneficiary at check-in and authorize the transaction with the provider at the point of service or check-out. This process, using a smart card with a PIN code, is known as two-factor authentication.

Medicare providers verify their identity and eligibility to provide services during an enrollment process. Currently, under the Affordable Card Act (ACA) high risk providers go through an enrollment process to verify their credentials and identity. Under the proposed Medicare CAC, each provider's identity is secured by supplying a biometric that will serve as their own unique key to their Medicare billing account. Providers receive a secure smart card which includes an embedded micro-processor that stores basic biographical information, their NPI, as well as their unique biometric key, thus binding the credential to the individual. The card and the biometric together authenticate the provider, similar to two keys used to open a safety deposit box (another type of two-factor authentication).

At the point of service, the transaction is authorized by both the provider and the beneficiary by creating an electronic verification between their two smart cards using the unique keys – in this case, the beneficiary's PIN code and the provider's biometric. This verification is critical as it creates a confirmation by both parties that the service was rendered. The two-factor authentication process (card plus PIN for beneficiaries and card plus biometric for providers) limits the ability of criminals to fraudulently bill Medicare by posing as a either a provider or beneficiary. It's important to note that this represents two major improvements over the current system: first, a successful transaction requires two parties, and second, each of those parties must provide two-factor authentication of their respective identities.

HOW MEDICARE CAC WORKS IN THE DOCTOR'S OFFICE



[Click here to visit the Secure ID Coalition's website and see a video of the process in action.](#)

HOW WILL MEDICARE CAC SOLVE THE PROBLEM?

Authenticating Identity of Beneficiaries, Providers and Suppliers

Unauthorized services and product transactions are essentially eliminated since both the secure smart card and the person who owns the key on the card are required to conduct the transaction. This means that phantom billing, fraudulent patient billing and stolen Medicare cards are no longer easy means of bilking Medicare. Furthermore, both parties to the intended transaction must verify the transaction. In addition to imposing strict anti-fraud mechanisms, a Medicare common access card would also reduce processing errors (duplicate or misdirected payments) through electronic verification of data and digitally signed electronic billing processes.

The Proposed Medicare Common Access Card does not call for use of biometrics for beneficiary authentication.

As discussed above, the proposal calls for patients to authenticate their identity via the Medicare CAC smart card and a unique PIN. Within the healthcare industry, biometrics are increasingly used for identification due to concerns about patient safety, identity theft, and insurance fraud.

While biometrics are among the most accurate identity verifiers, and are currently used to identify people in many diverse settings including amusement parks, airports, public schools, hospitals, retail outlets and federal government facilities, we are not recommending biometrics for Medicare or Medicaid beneficiaries at this time due to the significant challenges and costs of enrollment.

Authentication of Medicare Providers and Suppliers

Biometric authentication is recommended, however, for providers and suppliers in the Medicare CAC system. This would extend to billing agents within a doctor's office or hospital.

Biometrics is the science of identifying people based on certain unique physical characteristics. Examples of types of biometric identification include facial geometry, fingerprint, hand, retina and iris. As part of Medicare CAC, and in a secure smart card environment, biometric data is distilled to a mathematical calculation known as a *template*. Because the template is a representation of the biometric and not the actual image, it cannot be reproduced, copied or stolen. The biometric template is encrypted and securely stored inside the micro-controller embedded in the provider's smart card. At the point of verification, the card is placed in a card reader. No information on that card can be read until the biometric that was provided at enrollment is presented and read. The smart card and the reader would then perform a *one-to-one match* (also known as *match-on-card*) between the template on the card and the live

8

image. The biometric is confirmation that the person to whom the card belongs is present. Because no one would have the associated biometric except for the rightful individual, the system prevents fraudulent behavior. As a result, CMS is afforded the ability to use biometric authentication without maintaining an online national biometric database.

Some biometric systems require an online database to which images are matched when they are presented for verification. This process is called a *one-to-many match*. In the case of Medicare this approach is not recommended because there is no need to try to determine who is filing the claim, only a need to verify that the claim is being filed by the person authorized and to whom the card was issued. The one-to-many match requires constant online access to a central Medicare biometric database and is used to answer the “who is this” question. It would require providers to wait for verification of a one-to-many match process which can take significant time. Having a central Medicare biometric database accessible online is also an invitation for hackers and fraudsters to attempt to breach the system. A one-to-one or match-on-card system answers the “is the person I think it is” question of concern.

For a secure, authenticated Medicare system, a one-to-one match using biometric templates is the recommended approach, giving each provider complete control over their card and verification process. Making authentication easy and less time-consuming benefits both beneficiaries and providers.

Medicare Beneficiary Privacy and Security

A secure Medicare smart card strengthens beneficiary privacy and security in a number of ways. First, the beneficiary’s Social Security number (SSN), used today as the Medicare Claim Number, will no longer be printed on the card and readily available to identity thieves. The identification information is encrypted and stored safely on the secure embedded chip. Second, information on the card can only be read by an authorized Medicare card-reader, and only when the beneficiary consents to input their correct PIN code. Third, personal information is protected through encryption when transmitted electronically and when stored. The Medicare Common Access Card not only improves the patient’s privacy and security in a medical environment, but it strengthens the beneficiary’s overall privacy, reducing opportunities for identity theft and fraud.

Medicare Provider Privacy and Security

The secure Medicare smart card system similarly protects the privacy and security of the provider’s information. NPI’s and other personal information will no longer be printed on the front of the card; instead, it will be encoded on the card’s secure embedded chip. As with beneficiaries, only an authorized Medicare card reader system can access the information on the card, and then only when the provider has consented to present his biometric. These precautions not only protect the legal card holder’s privacy, but also ensure the integrity of the

system from fraudsters who steal a provider's card in order to make an unauthorized transaction.

Realizing that providers don't always file the claim to Medicare themselves, the Medicare CAC offers flexibility in that administrative personnel can also be equipped with a Medicare CAC card as an authorized representative of the provider after undergoing the same enrollment process as the provider. To file the claim, the provider's NPI would be securely stored on the authorized representative's smart card. This flexibility alleviates the need for providers to be present to file a claim, and presents no interruption in provider workflow.

Common Access Card: NIST Approved Open Standards

In the U.S., open standards for secure identity credentials such as the DOD CAC and PIV cards were developed collaboratively by industry standards organizations with the participation of the U.S. government through the National Institute for Standards and Technology (NIST). The NIST standards were jointly developed to protect both physical and logical (computer networks) government infrastructure against attack.

The Office of Management and Budget, through OMB M-11-11, mandated that every federal agency, including the Department of Defense, utilize secure smart cards to authenticate and verify users for building access and computer access. While it is hard to measure fraud within government agencies, the DOD confirms a 46% reduction in cyber security attacks on the first day of secured logical access implementations in any given department. The U.S. e-Passport is based on the same underlying secure identification technology and was implemented to prevent unauthorized access into the United States.

WHAT ARE THE BENEFITS OF A MEDICARE SMART CARD TO BENEFICIARIES, PROVIDERS AND TAXPAYERS?

Benefits to Beneficiaries

A secure Medicare smart card strengthens beneficiary privacy and security in a number of ways.

- **Social Security Number Removed From Front of Medicare Card**
The beneficiary's Social Security number (SSN) is no longer printed on the card and readily available to identity thieves. The identification information will be stored safely on the secure embedded chip.
- **Beneficiary Consent**
Information on the card can only be read by an authorized Medicare card-reader, and only when the beneficiary consents to input their correct PIN code.

- **Personal Information is Encrypted**
Personal information is protected through encryption when transmitted electronically and when stored.
- **More Funds Available for Legitimate Care**
Reduction in fraud within the system makes more funds available for legitimate healthcare needs of Medicare beneficiaries.

Benefits to Providers and Suppliers

A secure Medicare smart card strengthens providers' privacy and security in a number of ways and enables more efficient business practices.

- **Quicker Processing of Payment**
Because transactions are verified by both the provider and beneficiary a non-repeatable audit trail is created. This electronic processing eliminates paperwork and streamlines to payment cycle, allowing for quicker and more accurate payment to providers.
- **Billing Accuracy**
In many cases claims are rejected because of small mistakes or typos. Because the chips verify both the provider and beneficiary all information is electronic, eliminating these types of mistakes.
- **Reduces Need for Recovery Audit Contractors**
Because both beneficiaries and providers provide proof they are legitimate, payment is pre-approved before it is sent, reducing the need for backend recovery audit contractors.
- **Streamlined Processes Increase Administrative Efficiency**
Smart cards store basic patient and beneficiary information on the secure chip. That information can be accessed by the provider at point of check-in to identify the correct patient record and eliminate many of the administrative check-in procedures.
- **Protects Medicare Provider Numbers**
Today provider numbers are widely available and used by thieves billing Medicare for products and services never performed. Using a smart card guarantees that no one can masquerade as the provider and use their number to bill Medicare.
- **Traceability/Audit trail**
Using a smart card as part of the billing process creates an unrepeatable audit trail definitively verifying the details of each transaction between beneficiary and provider. Since the information is electronically signed and transmitted to CMS processing the information cannot be changed, altered or hacked.

Benefits to Taxpayers

While both beneficiaries and providers receive protections and benefits within the system, taxpayers ultimately gain the most significant benefit: reduction of fraud, waste and abuse within the Medicare system. Taxpayer funds can now be targeted directly to those Americans entitled to Medicare benefits, without fear of siphoning by crooks. Such a program will go a

long way towards providing stability and restoring integrity in a program on which so many Americans rely.

WHERE HAS THIS TYPE OF PROGRAM BEEN SUCCESSFUL?

Smart cards are used in the US and around the world to prevent fraud and reduce costs. Below are just a few examples of smart card deployment that have resulted in significant savings.

US Healthcare

While there are myriad examples of smart card implementations in healthcare across the US, we've chosen to highlight two showing cost savings for both large and small hospitals alike.

- Mt. Sinai Hospital, New York City. When Mt. Sinai deployed smart cards to their patients to reduce the number of duplicate or overlaid records in their system, estimated to be close to 15%. The hospital was able to eliminate annual large scale medical record clean-ups which cost the institution \$1.8 million and involved over 250,000 duplicate records. Additional benefits included the elimination of the patient clipboard paperwork and reduction in medical errors.
- Memorial Hospital, North Conway, New Hampshire. Memorial Hospital reduced admission errors from 6% of patient records to less than 1% by deploying smart cards, including the reduction of medical record error from a rate of 7% to less than 1%, creating an annual savings of \$55,000 for a 35 bed hospital. Patients saw a direct benefit as Memorial Hospital was able to reduce their admission time from 22 minutes to less than 3 minutes – an immediate cost savings of \$574,000 in annual employee payroll minutes, which allowed Memorial to redirect staff to other productive tasks.

International Healthcare

A number of nations have implemented smart card-based healthcare systems for many reasons beyond fraud reduction, such as security and ensuring administrative cost savings.

- French healthcare system SESAM-Vitale. The French government implemented smart cards in order to verify who was receiving treatment and to quickly provide reimbursements within three to five days as opposed to 3-4 weeks. As a result, the processing cost of a claim within the system was reduced from 1.74 Euros to .27 Euros. With over one billion transactions per year, the transition saves the system over 1.4 billion Euros/year.
- German Ministry of Health. Germany deployed secure smart healthcare cards to approximately 70 million beneficiaries and is currently deploying about 280 thousand health professional cards. The projected achievable program savings in the German national program range from 1.7 to 2.9 billion Euros per year, of which between 800

12

million to two billion Euros would come from fraud reduction. According to the German Ministry of Health in January 2012, the beneficiary deployment alone has generated annual fraud reduction of 250 million Euros. Provider fraud reduction data will not be available until deployment is completed next year.

- Taiwan. The Taiwanese government implemented one of the longest standing and most comprehensive secure health care cards in the world. Implemented in 2004, the program has issued 24 million patient cards and 300 thousand provider cards. The card data includes not only insurance information but medical information as well. The Bureau of National Health in Taiwan reports that moving from paper to a secure smart card has extended the life of cards by 5-7 years, reduced fraud, saved on administrative costs, and reduced health care spending in general. Taiwan's administrative costs are the lowest in the world at two percent (compared to the U.S. at 31 percent).

Financial Services

The smart card technology present in the proposed Medicare CAC Act has been used to great success across the globe to protect identity and secure transactions not only in health care, but in the financial services market as well. Known as "Chip & PIN", the smart card technology has revolutionized the way banks have reduced fraud and identity theft. Examples of success include:

- United Kingdom Chip & PIN smart card deployment for credit and debit card market. According to a UK Payments Administration reported in 2010, overall fraud losses in the UK fell by 67% and counterfeit card fraud losses have decreased by 77% since 2004, when Chip & PIN was adopted.
- France's Chip & PIN smart card deployment for credit and debit card market. The French banking association GIE CB reported in November 2010 that a fraud ratio of 0.072%, for a total 350 million (USD) – of which \$140 million (USD) originated outside France. Five years ago 26% of the system wide fraud was attributed to the Internet and 74% attributed to the real world. Today the numbers are exactly the opposite with 75% attributed to Internet fraud and 25% to real world. GIE CB credits smart cards with reducing real world fraud. For a frame of reference, over 3.5 billion smart card transactions occur every year for a value of \$597 billion (USD). There are 58 million smart banking cards in circulation in France (population 64m) with an average of 113 operations/transactions per user.

A trusted privacy and security tool for the Federal government

In addition to helping reduce fraud costs around the world, smart cards have been a reliable resource throughout the federal government for identity management and security for more than a decade. Designed on open standards approved by NIST, smart cards use non-proprietary technologies to help secure American's identity and security both home and abroad. Current federal smart card applications include:

- The Department of Defense Common Access Card. Today every federal agency, including the Department of Defense, utilizes secure smart cards to authenticate and verify users for building and computer access. While it is hard to measure fraud within government agencies, the DOD confirms a 46% reduction in cybersecurity attacks on the first day of secured computer access implementation.
- The ePassport. Developed by the State Department and the Government Printing Office, all new passports include a secure smart card computer chip embedded in the back cover. Included to thwart passport counterfeiters, the secure chips protect American citizen's personal information in a manner that prevents tampering and eavesdropping. Since the first year of deployment, 2005, the State Department issued over 75 million ePassports containing the secure smart card chip.
- The Federal Emergency Management Agency's First Responders Authentication Credential (FRAC). In order to ensure local and state emergency response officials are able to collaborate to ensure the public's safety, many identity management challenges must be overcome. The FRAC card meets the task by allowing for interoperability between local, state, and federal first responders. So far, nine states have taken the lead to deploy FRAC credentials for first responders, with many more on the way. It should be noted that all doctors and nurses are considered first responders; as such a Medicare CAC provider card could serve double duty as a FRAC credential, even further reducing implementation costs.
- The American Medical Association/Centers for Disease Control Health Security Card. The American Medical Association's Center for Public Health Preparedness and Disaster Response is working with Center for Disease Control and FEMA to develop a pilot program to show the benefit of a Health Security Card based on smart card technology for patients in the event a disaster or health emergency. Preliminary findings from the pilot excises show 90% of patient using the smart cards rated the care they received as good to excellent, with 75% affirming care as very good or excellent. In December the AMA will issue a final report on the smart card pilot.

WHAT ARE THE COSTS OF IMPLEMENTING MEDICARE CAC?

Recently, the Smart Card Alliance, an industry non-profit 501 (c)(3) education foundation and trade association, worked with an independent auditor to determine the cost of deploying a smart card based Medicare card system for both providers and beneficiaries (*see attached, DeLeon & Stang Medicare Report*). The audit was completed in March 2012 with the intent to assist Congress and the Centers for Medicare and Medicaid Services in their efforts to understand the true cost and actual savings of a nation-wide Medicare CAC deployment.

The audit found there are many different elements that must be considered as part of a national Medicare CAC deployment. Because the system will determine real-time eligibility of

14

both providers and beneficiaries, it requires more than just the use of a smart card. Backend infrastructure and readers must be accounted for in any cost estimate. The estimate accounts for 2.6 million providers and 48 million beneficiaries for an overall total of 50.6 million participants.

Because providers will be going through an enrollment process and their biometric information will need to be captured the cost per provider within the system is estimated to be \$31.08 per provider. For the beneficiary, the cost is somewhat less, \$14.57 per beneficiary, because the beneficiary will receive their smart card via U.S. mail without the requirement of enrollment of biometric capture. The PIN code for the beneficiary could come pre-set as the last four digits of their Social Security number and could easily be changed, if the beneficiary desired upon first use. The total cost for nationwide deployment of Medicare CAC system averages out to \$24.24 per participant for a grand total of \$1.3 billion for full deployment. These costs are completely inclusive for full deployment and should be evaluated against the return in reductions in fraud, waste and abuse.

WHAT IS THE RETURN ON INVESTMENT AND WHAT IS IT BASED ON?

The Department of Justice estimates that fraud within the Medicare system costs American taxpayers over \$60 billion per year. According to the General Accountability Office (GAO) in 2010 improper payments within Medicare were \$48 billion per year. Senator Tom Coburn (R-OK) provided estimates during a March 2, 2011 Senate Finance Committee hearing entitled *Preventing Health Care Fraud: New Tools and Approaches to combat Old Challenges*, fraud and improper payments in the Medicare and Medicaid programs to cost taxpayers between \$100 billion - \$120 billion per year. Looking at the problem from any prospective, there is a lot of money at stake.

Based on savings reported by the UK, France, Germany and Taiwan across both the healthcare and financial services industries (noted above), it is clear that the use of smart card-based solutions led to a reduction in overall fraud losses upwards of 70%. While the Secure ID Coalition believes that the smart card-based Medicare CAC program will be able to deliver similar results, it is entirely reasonable to assume – at the very least – a cost savings of at least 50%, representing well over \$30 billion in eliminated fraud annually at the current rate of fraud. This conservative estimate is further reinforced by the DOD's confirmation of a 46% reduction in cybersecurity attacks on the first day of deployment of the CAC card for computer access.

RECOMMENDATIONS

- Because the Medicare program is unique, deploying pilot programs or demonstration projects will be an important part of any successful smart card implementation. Five pilot projects in areas where there is a significant amount of fraud will help to identify the specific needs of the Medicare community. These areas could include specific states or regions, similar to metro regions, prioritized by risk categories.
- Planning is a critical part of any pilot program. It is the recommendation of the Secure ID Coalition that the Secretary of HHS be given enough time to plan for the success of the pilots, with a minimum of one year for mapping prior to implementation. Within the mapping period a process by which HHS/CMS establishes metrics to quantify reductions in fraud, waste and abuse must be clearly defined. Further, details of how beneficiary and provider privacy will be protected must be addressed.
- Assuring the interoperability of the new Medicare CAC hardware with existing practice management software systems will also be an important part of the pilot program. Claims are increasingly submitted through electronic interfaces; when including authenticated receipts of rendered services from the new Medicare CAC hardware, claims will be easier to verify by CMS, thus further reducing fraudulent payments and expediting audits. Since the private sector is tasked with the development and implementation of these practice management (PM) systems, the pilot program should be developed to report the essential data needed for determining how best to integrate Medicare CAC hardware into daily medical management practices.
- In order for pilots to provide the requisite amount of data, detailed information about usability, and specific measurable costs and benefits, a minimum duration of eighteen months is recommended for the pilot programs.
- Success of the pilot program will be determined by the established metrics defined prior to the start of the pilot program. Once completed HHS/CMS will be able to verify potential cost savings and benefits and determine the viability of a nationwide deployment without further direction from Congress.
- Once the pilots are completed, HHS/CMS will be able to assess the pilot data and design a nationwide Medicare smart card program that meets the needs of providers, beneficiaries and tax payers.
- Implementing a nationwide program of this scope should be done methodically and over time as to not overload HHS/CMS.

CONCLUSION

It's everyone's desire to see both the Medicare and Medicaid programs not only survive, but thrive. The cost of waste, fraud and abuse in these systems not only eat away at our tax reserves, but also forces federal and state authorities to spend tens of millions of dollars every year in law enforcement and prosecution costs. It only makes sense to stop the fraud before it happens. In this case, that means implementing a secure smart card to verify and authenticate valid Medicare and Medicaid users at the time of the transaction.

Smart cards are not only a globally recognized tool to help eliminate medical and financial fraud, but a trusted tool of the federal government in assuring identity across a number of critical applications. If Congress were to implement a smart card technology solution – such as described in the Medicare Common Access Card Act – it would have the potential to save American taxpayers over half of the estimated \$60 billion per year cost of fraud. With over 48 million seniors, that comes out to approximately \$1,250 of fraud per recipient per year. However, for a one-time investment of less than \$25 per beneficiary, the federal government will realize a cost savings of over \$612.50 per beneficiary per year – a return on investment 24 times over.

The Secure ID Coalition stands ready to assist Congress in helping save the Medicare and Medicaid programs. We look forward to working with you and answering any questions you may have.

QUESTIONS & ANSWERS

If the beneficiary does not have their card, will they be denied access to care?

Absolutely not. CMS will need to establish a policy for how to process claims that are outside of the validated and authenticated Medicare CAC system.

Some cards will get lost, whether it's because of illness or just plain forgetfulness; it happens today in every program. This is not a technology issue, but a question of policy on how CMS would treat billings that have not been authenticated. In the case of beneficiaries who need to have a caretaker or legal guardian tend to their medical needs because they cannot communicate, a special caretaker credential could be issued to them.

How will personal privacy be protected using a smart card?

Both privacy and security must be considered fundamental design goals for any personal ID system and must be factored into the specification of the ID system's policies, processes, architectures, and technologies. The use of smart cards strengthens the ability of the system to protect individual privacy and secure personal information.

Unlike other identification technologies, smart cards can provide authenticated and authorized information access, implementing a personal firewall for the individual and releasing only the

17

information required when the card is presented. Smart card technology provides strong privacy-enabling features for ID system designers, including the ability to:

- Support anonymous and pseudonymous schemes
- Segregate multiple applications on the card
- Support multiple single-purpose IDs
- Provide authentication of other system components
- Provide on-card matching of cardholder verification information
- Implement strong security for both the ID card and personal data

Smart cards trust nothing until proven otherwise. For example, smart cards can require cardholders to authenticate themselves first (with a PIN or biometric) before the cards will release any data. And smart cards support encryption, providing patient data privacy and enabling at-home or self-service applications in suspect or untrusted environments to be secure.

The smart card's embedded secure microcontroller provides it with built-in tamper resistance and the unique ability to securely store large amounts of data, carry out own on-card functions (e.g., encryption and digital signatures), and interact intelligently with a smart card reader.

In case a beneficiary card is lost, how secure is one's personal information?

If the card is lost, the data on the card is secure and not readable without the individual's PIN code. Further, all information stored in the card cannot be read unless accessed via an authorized, authenticated reader. An attempt to hack the chip on the card would destroy the information in the process, because the chips are designed to shut down under brute force attacks. Once the card is reported lost or stolen the system will no longer recognize it and it becomes completely useless. One of the significant benefits that will reduce medical ID theft is that the card will no longer have the beneficiary's social security number printed on it.

In the case of beneficiaries seeking care outside their home region, how will the cards work?

This is an issue that exists today with paper Medicare cards containing SSNs in full view. The secure Medicare smart cards will work in any authenticated provider reader and benefits will be fully available nation-wide under existing Medicare services guidelines. During the pilot program, CMS would treat beneficiaries seeking care outside their home region under the same policies as if the beneficiary had lost their card.

Would a smart card program work with other program integrity efforts CMS has already deployed?

A smart card program will complement existing programs initially and, over time, the SIDC anticipates CMS would do away with some of the reactive initiatives underway due to the success of the smart card program to reduce fraud, waste and abuse in the system. Unlike the programs currently underway that search for fraud after the transaction has been processed and the money disbursed, the smart card program is a proactive fraud prevention approach. To date, no proactive initiatives have been put forth by CMS.

APPENDIX

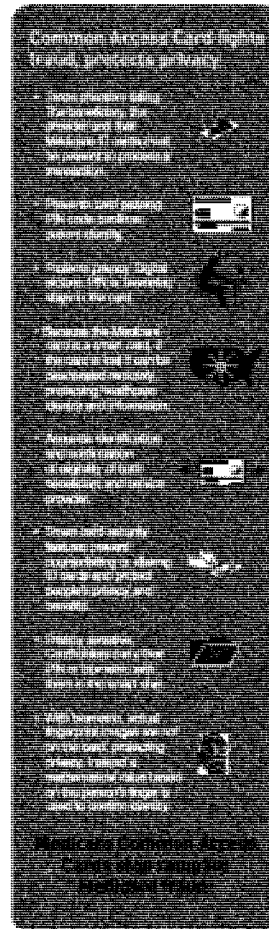
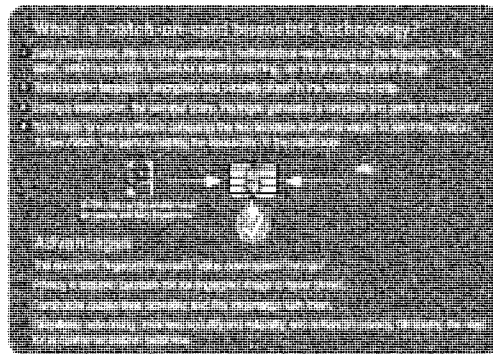
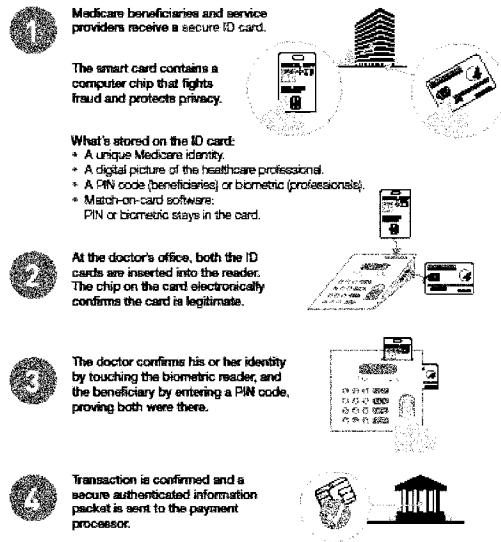
ADDITIONAL RESOURCES

- Smart Cards and Biometrics in Healthcare Identity Applications, Smart Card Alliance Healthcare Council white paper, May 2012
- Benefits of Smart Cards versus Magnetic Stripe Cards for Healthcare Applications, Smart Card Alliance Healthcare Council brief, December 2011
- Effective Healthcare Identity Management: A Necessary First Step for Improving U.S. Healthcare Information Systems – A Smart Card Alliance Brief for Government Policy Makers and Other Stakeholders, Smart Card Alliance Healthcare Council and Identity Council brief, March 2009

ATTACHED DOCUMENTS

- Secure ID Coalition, *Medicare Common Access Card: How Does It Work*, 2012.
- DeLeon & Stang Certified Public Accountants and Advisors, *Smart Card Alliance Projected Schedule of Costs To Deploy Secure ID Card and Related Fraud Reduction Cost Savings and Return on Investment with Independent Accounts' Report*, June 27, 2012.
- AARP Joins Bipartisan Effort to Prevent Identity Theft of Medicare Beneficiaries, September 14, 2011.
- Lawrence Carbonaro, *Converting to LifeMed*, Memorial Hospital of Conway, New Hampshire, 2012. (Memorial Hospital report on savings realized from conversion to LifeMed, a smart card-based health information system.)
- Theresa Min-Hyung Lee, *Comparative Study of Taiwanese Health Care System*, in The Ampersand Journal, Issue IV 42 (McGill University), 2011.

How it works Medicare Common Access Card



**SMART CARD ALLIANCE
PROJECTED SCHEDULE OF COSTS
TO DEPLOY SECURE ID CARD
AND RELATED FRAUD REDUCTION COST
SAVINGS AND RETURN ON INVESTMENT
WITH
INDEPENDENT ACCOUNTANTS' REPORT**





100 Lakeforest Boulevard
Suite 650
Gaithersburg, MD 20877
P: 301-948-9825
F: 301-948-3220
www.deleonandstang.com

Allen P. DeLeon, CPA, P.C.
Richard C. Stang, CPA, P.C.
Jennie Price

INDEPENDENT ACCOUNTANTS' REPORT

Smart Card Alliance Washington, DC

We have examined the accompanying projected Schedule of Costs to Deploy a Secure ID Card Within the U.S. Medicare System, and the Schedule of Projected and Fraud Reduction Cost Savings of Deployment of a Secure ID Card Within the U.S. Medicare System and the Related return on Investments (ROI) as of February 13, 2012, which has been prepared by Smart Card Alliance. Smart Card Alliance's management is responsible for the projections, which were prepared for the purpose of providing educational information relevant to proposed legislation being drafted by the U.S. Congress. Our responsibility is to express an opinion on the projections based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included such procedures as we considered necessary to evaluate both the assumptions used by management and the preparation and presentation of the projection. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, the accompanying projections are presented in conformity with guidelines for presentation of a projection established by the American Institute of Certified Public Accountants, and the underlying assumptions provide a reasonable basis for management's projections assuming:

1. The deployment costs are accurately projected by using an average of the projected deployment costs based on a survey of six companies which specialize in deployment of similar secure ID cards for similar purposes in the U.S. and foreign countries, and other estimates of deployment costs made by the Smart Card Alliance, Health Council Members.
2. The quantity of projected users of the secure ID card are accurately estimated using U.S. Department of Health and Human Services (HHS) information as described in the projection.
3. The cost savings are accurately projected by using cost savings of similar programs in the U.S. and foreign countries, as described in the projection.
4. The return on investment (ROI) is accurately projected by using the projected cost savings and applying it to the estimated current levels of Medicare fraud.

However, even if the assumptions referred to above are accurate, there will usually be differences between the projected and actual results, because events and circumstances frequently do not occur as expected, and those differences may be material. We have no responsibility to update this report for events and circumstances occurring after the date of this report.

The accompanying projection and this report are intended solely for the information and use of (1) members of management of the Smart Card Alliance and (2) the U.S. Congress and related US government agencies, in connection with proposed legislation related to the deployment of secure ID cards, and are not intended to be and should not be used by anyone other than these specified parties.

DeLeon & Stang
DeLeon & Stang, CPAs and Advisors
Gaithersburg, Maryland
June 27, 2012

...improving the financial lives of our clients, our staff & our community with integrity, trust & innovation.

SMART CARD ALLIANCE
Schedule of Costs to Deploy a Secure ID Card
Within the U. S. Medicare System
February 13, 2012

National Rollout

Professionals working at hospitals, physician's offices.
 Medical equipment suppliers, nursing homes, assisted living
 residences, mental health professionals and pharmacies who
 require ID cards.

Quantity	Source of information
TOTAL PROFESSIONALS	2,624,884 National Pin and provider Enumeration System Statistics 5'05 - 7'11

Cards Required	Quantity	Price Per Unit	Total	
Professionals	2,624,884	\$4.17	\$10,932,642	See quantity above
Beneficiaries	48,091,000	\$1.04	\$48,091,200	Industry estimate
TOTAL CARDS	50,624,884	\$1.17	\$59,023,842	

Medicare Cost Summary

Providers and Suppliers	Users	Average Cost Per Person	Total	Comments
Enrollment of Providers and Suppliers	2,624,884	\$12.83	\$33,637,888	Cost to enroll everyone, prove licensing
Background Investigation (Vetting)	2,624,884	\$9.00	\$23,623,956	Already included in existing processing costs
BioMetric AFIS Database	2,624,884	\$9.59	\$25,157,869	Checking against data base
Large Systems Integrator (LSI)	2,624,884	\$0.76	\$1,994,912	Allow cards to be read in existing CMS system
Digital Certificate - Level 3 MHW Assurance	2,624,884	\$1.01	\$2,638,008	Electronic version of ID recognition
Card Stock	2,624,884	\$4.17	\$10,932,642	Physical card from above
Card Issuance & Fulfillment	2,624,884	\$3.23	\$8,522,123	Mailing out cards
Card Manufacturer Professional Services	2,624,884	\$0.10	\$262,488	Consulting
Middleware/ Strong Authentication Server with Connect	2,624,884	\$6.62	\$17,363,688	Connect to software
Software Licensing	2,624,884	\$1.25	\$3,283,730	Licensing of vendor software
Card Management System (CMS)	2,624,884	\$9.33	\$24,488,087	Integration
Identity Management System (IDMS)	2,624,884	\$9.21	\$24,188,101	Integration
PROVIDER & SUPPLIER TOTAL	2,624,884	\$31.08	\$81,584,457	

SMART CARD ALLIANCE
Schedule of Costs to Deploy a Secure ID Card
Within the U. S. Medicare System
February 13, 2012 (Continued)

Beneficiaries	Users	Per Person	Total	
Digital Certificate plus Class 2 Identity Proofing	48,000,000	\$2.82	\$135,200,000	PIN required to activate
Card stock	48,000,000	\$1.00	\$48,000,000	Electronic version of ID recognition
Card Issuance & Fulfillment	48,000,000	\$3.14	\$150,720,000	Physical card from above
Card Manufacturer Professional Services	48,000,000	\$0.07	\$3,360,000	Mailing via cards
Middleware/ Strong Authentication Server with Connect	48,000,000	\$0.23	\$11,040,000	Consulting
Large Systems Integrator (LSI)	48,000,000	\$5.24	\$251,520,000	Connect to software
Software Licensing	48,000,000	\$1.26	\$60,720,000	Licensing of vendor software
Card Management System (CMS)	48,000,000	\$0.32	\$15,360,000	Integration
Identity Management System (IDMS)	48,000,000	\$0.21	\$10,080,000	Integration
BENEFICIARY TOTAL	48,000,000	\$14.57	\$699,542,400	
Readers and Terminals	Quantity	Per Unit/Per Person	Total	
USB Contact Readers	170,537	\$7.50	\$1,279,028	
Dual Skined Terminals (German model)	103,000	\$162.50	\$16,737,500	
Biometric (Fingerprint) Readers	170,537	\$80.00	\$13,642,933	
	444,073	\$71.29	\$31,659,458	
Activation Kiosks	17,500	\$23,666.61	\$414,165.67	To change PIN, add photo, activate card
GRAND TOTAL (National Rollout)	60,624,884	\$24.24	\$1,226,951,990	
Annual Maintenance of Total Cost		2.5%	\$306,737,997.60	% of total costs estimate

SMART CARD ALLIANCE
Schedule of Projected Fraud Reduction Cost Savings of
Deployment of a Secure ID Card in the U. S. Medicare System
And the Related Return on Investments

Fraud	Year 1	5 Yr. aggregate	10 yr. aggregate
Current Situation	\$60,000,000,000	\$300,000,000,000	\$600,000,000,000
Fraud Reduction Percentage	Savings		
10%	\$6,000,000,000	\$30,000,000,000	\$60,000,000,000
20%	\$12,000,000,000	\$60,000,000,000	\$120,000,000,000
33%	\$19,800,000,000	\$99,000,000,000	\$198,000,000,000
40%	\$24,000,000,000	\$120,000,000,000	\$240,000,000,000
50%	\$30,000,000,000	\$150,000,000,000	\$300,000,000,000
66%	\$39,600,000,000	\$198,000,000,000	\$396,000,000,000
70%	\$42,000,000,000	\$210,000,000,000	\$420,000,000,000
80%	\$48,000,000,000	\$240,000,000,000	\$480,000,000,000
90%	\$54,000,000,000	\$270,000,000,000	\$540,000,000,000
Return on Investment			
Fraud Reduced by			
10%	\$4,466,310,012	\$27,239,358,022	\$55,705,668,034
20%	\$10,466,310,012	\$57,239,358,022	\$115,705,668,034
33%	\$18,266,310,012	\$96,239,358,022	\$193,705,668,034
40%	\$22,466,310,012	\$117,239,358,022	\$235,705,668,034
50%	\$28,466,310,012	\$147,239,358,022	\$295,705,668,034
66%	\$38,066,310,012	\$195,239,358,022	\$391,705,668,034
70%	\$40,466,310,012	\$207,239,358,022	\$415,705,668,034
80%	\$46,466,310,012	\$237,239,358,022	\$475,705,668,034
90%	\$52,466,310,012	\$267,239,358,022	\$535,705,668,034

SMART CARD ALLIANCE
Project Deployment Costs and Fraud Reduction Savings of Secure ID Card
February 13, 2012

NOTE 1 - NATURE AND PURPOSE OF ORGANIZATION

The Smart Card Alliance is a non-profit organization, located in Washington DC and tax exempt under section 501 (c) (6) of the Internal Revenue Code (IRC). Its mission is to accelerate the widespread adoption, usage and application of smart card technology in North America, by bringing together users and technology providers in an open forum to address opportunities and challenges for the industry. Its membership consists of companies and individuals in technology companies, federal, state and local governments, academic institutions, consulting companies and Latin American companies and institutions. The Organization conducts conferences, prepares publications, and provides resources to its members in furtherance of its purpose.

NOTE 2 - SPECIFIC PURPOSE OF THE PROJECTIONS

The purpose of this report is to provide projections related to (1) the estimated costs of the deployment of a secure ID card in the U.S. Medicare system to the U.S. Congress, (2) the estimated fraud reduction cost savings and return on investment (ROI), in relation to proposed legislation to conduct a pilot program.

NOTE 3 - UNDERLYING ASSUMPTIONS USED ON THE PROJECTIONS

Certain assumptions were used in developing the projections. The projections are only as reliable as the accuracy of the assumptions. Even if the assumptions described in this report are accurate, there will usually be differences between projected results and actual results, because events and circumstances frequently do not occur as expected and those differences could be material. The underlying assumptions used to develop the projections in the report are:

1. The costs of deployment of a secure ID card are based on the average cost projections developed from a survey of technology companies which are members of the Smart Card Alliance. The survey consisted of six companies, and the projected costs are an average of the costs projected by these companies. Some companies did not provide cost information in all cost areas. Some of the estimates of deployment costs were made by the Smart Card Alliance and Healthcare Council Members, and not directly from the survey results. The surveyed companies; cost projections are only as accurate as the projections provided by the survey. Since the overall deployment costs are based on the cost per user multiplied by the number of projected users, the actual deployment costs could differ significantly from the projected costs if the actual cost per user is different from the projected cost per user.

SMART CARD ALLIANCE
Project Deployment Costs and Fraud Reduction
Savings of Secure ID Card (Continued)
February 13, 2012

NOTE 3 - UNDERLYING ASSUMPTIONS USED ON THE PROJECTIONS (Continued)

2. The quantity of projected users of the secure ID card was determined from information obtained from the National Plan and Provider Enumeration System (NPPES), a division of the Centers for Medicare and Medicaid Services (CMS) of the U. S. Department of Health and Human Services (HHS). Since the projected costs of deployment of a secure ID card is based on the cost per user multiplied by the number of projected users, the accuracy of the number of users is a material component in the total cost projection. The NPPES information is generally considered to be the most current and accurate estimate of the number of users of a secure ID card. However, the overall deployment costs relies heavily on the quantity of users, and may differ significantly from the actual costs if the actual number of users differs from the projected number of users.
3. The fraud reduction cost savings is presented at various assumed percentages of savings. It is assumed that the current Medicare fraud is approximately \$60 billion per year. The fraud reduction cost savings is based on cost savings of similar programs using other applications of the secure ID card and deployment of a secure ID card in other countries whose medical systems and related regulations differs from those in the U.S. While management believes that the fraud reduction cost savings reported by other secure card applications and deployments in other countries is a reasonable estimate of the fraud reduction cost savings that would be achieved in the U.S., material differences could exist which would affect the total cost savings.
4. The projected return on investment (ROI) is also presented at various assumed fraud reduction percentages. The projected ROI is computed by subtracting the total projected fraud cost savings, at each assumed savings percentages, from the projected deployment costs. Since the total projected deployment costs and the projected fraud reduction savings are based on the assumptions described above, the ROI is based on, and subject to, these assumptions. If the total projected deployment costs and/or the total projected cost savings differ materially from the actual results, the actual ROI will differ materially from the projected ROI.

SMART CARD ALLIANCE
Project Deployment Costs and Fraud Reduction
Savings of Secure ID Card (Continued)
February 13, 2012

NOTE 4 - LIMITATIONS OF USE OF THE PROJECTIONS AND SPECIFIED PARTIES

The projected information contained in this report is intended for a specific purpose and use, it is not intended that the projections be used for any other purposes or uses. Further, this report is intended for use by (1) Members of the Smart Card Alliance, (2) the U.S. Congress and related U. S. government agencies related to proposed legislation concerning a pilot program for deployment of a secure ID card in the U.S. Medicare system, the use of this report is not intended to be used, and should not be used, by any other parties other than the specified users.



AARP Joins Bipartisan Effort to Prevent Identity Theft of Medicare Beneficiaries

AARP today endorsed the Medicare Common Access Card Act of 2011

From: [Press Center](#) | September 14, 2011

FOR
September 14, 2011

IMMEDIATE

RELEASE

CONTACT:
AARP Media Relations, 202-434-2560

AARP Joins Bipartisan Effort to Prevent Identity Theft of Medicare Beneficiaries

WASHINGTON – AARP today endorsed the Medicare Common Access Card Act of 2011 in a letter to U.S. Senators Mark Kirk and Ron Wyden as well as U.S. Representatives Jim Gerlach and Earl Blumenauer. The bill will create a secure Medicare identification card pilot program for beneficiaries located in five geographic areas nationwide. This bipartisan and bicameral piece of legislation introduced today will replace paper Medicare cards with secure cards that carry the personal information electronically of individuals in the program.

Excerpts of the letter of support from Joyce A. Rogers, AARP Senior Vice President, are below:

“On behalf of AARP’s millions of members, we are pleased to endorse the Medicare Common Access Card Act of 2011. Your legislation will create a secure card pilot program under the Medicare program.

“Older Americans are particularly vulnerable to the dangers of identity theft. Your legislation will pilot a program to replace the current paper Medicare card with a smart card that would store the beneficiary’s personal information electronically on a computer chip, and would require both beneficiaries and providers to confirm receipt of services at the time services were provided. Similar technology currently exists for Department of Defense personnel.

“Your legislation not only provides enhanced information security, but will also help to reduce fraud in the Medicare program by verifying the identity of both Medicare beneficiaries and providers. Medicare dollars should be spent on necessary services and not lost to fraudulent activities.”

29

For a copy of the full-text of the letter, please contact AARP Media Relations by phone at (202) 434-2560 or via email at media@aarp.org.

About

AARP is a nonprofit, nonpartisan organization with a membership that helps people 50+ have independence, choice and control in ways that are beneficial and affordable to them and society as a whole. AARP does not endorse candidates for public office or make contributions to either political campaigns or candidates. We produce AARP The Magazine, the definitive voice for 50+ Americans and the world's largest-circulation magazine with nearly 35 million readers; AARP Bulletin, the go-to news source for AARP's millions of members and Americans 50+; AARP VIVA, the only bilingual U.S. publication dedicated exclusively to the 50+ Hispanic community; and our website, [AARP.org](http://www.aarp.org). AARP Foundation is an affiliated charity that provides security, protection, and empowerment to older persons in need with support from thousands of volunteers, donors, and sponsors. We have staffed offices in all 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands.

AARP:

<http://www.aarp.org/about-aarp/press-center/info-09-2011/aarp-joins-bipartisan-effort-to-prevent-identity-theft-of-medicare-beneficiaries.print.html>



Converting to LifeMed

By: Lawrence Carbonaro
Director, Purchasing, Patient Access & HIS

The Memorial Hospital, North Conway, NH (35 beds, 100,000 annual patient visits and over \$300,000 in administrative savings annually, not including the marketing advantages)

- Decreased admissions error rate from 6% to less than 1%** *We average 1500 registrations a week, thus 90 records that used to require manual intervention to fix before billing; with LifeMed we no longer require that effort.)*
- Elimination of clip board and paper** *(We went paperless as a result of LifeMed. We used to print a cover sheet to give to the patient with each registration, this is no longer required. 156 cases of paper plus toner are no longer used, no shredding or storage.)*
- Reduced duplicate records from 7% to less than 1%** *(an annual cost savings of \$35K-\$55k for scrubbing records. No numbers reported for medical errors due to incorrect chart)*
- Reduced admission time from 22 minutes to less than 3 minutes** *(average salary equaling \$18.13 an hour and a average saving of 19 minutes equals a soft cost saving of \$5.74 per patient times 100,000 patients annually. Registration saving of \$574,000 of annual employee payroll minutes allowing Memorial to redirect staff to other productive tasks, like accurate insurance billings, etc. - LifeMed soft projection). See reduced staff below*
- Reduced medical record error from 7% to less than 1%** *(unreported cost savings but includes billing losses, medical procedure losses, medical errors, lawsuits, etc)*
- Reduced PAC System errors to less than 1%** *(Hard to quantify but PACs errors were occurring about 150 annually, now they are rare. Pacs administrator time was 3+ hours to fix each error. About \$25K savings, assumed pay would be greater than \$100K)*
- Reduced full time staff requirements from 21 to 15** *(Annual savings equates to \$224,640 using a burdened salary of \$37,440 annually).*
- Decreased insurance A/R from 55+ to 42 days** *(unreported saving; Current days are still reducing in A/R and is now below 41 days).*
- Increased Press-Ganey patient satisfaction by 10% within first 60 days** *(Memorial's now in the top 5% of all hospitals with satisfaction in registration - this was a major issue as our patient dissatisfaction began at admission even before the patient saw an employee or clinician. Patient satisfaction influenced patient and employee retention and employee gratification).*

Areas of Savings not reported or financially measured as of the date of these Administrative Measures:

- Patient Satisfaction Increase
- Diminished Registration Errors
- Diminished in Duplicate Records
- Diminished in Record Errors
- Elimination of Registration Paper
- Decreased Insurance A/R

Comparative Study of Taiwanese Health Care System

Theresa Min-Hyung Lee

The health care system of Taiwan is an exemplary model of how modern health care reform and major policy changes can bring about high quality universal health coverage to a country in a relatively short period of time. After years of consulting international experts in the health policy field and studying numerous health care systems around the world, Taiwan instituted its universal National Health Insurance (NHI) program in 1995, extending a comprehensive benefits package ranging from doctor visits, prescription drugs to even traditional Chinese medicine to 99 percent of the Taiwanese population. The Taiwanese receive their health care services in a very timely manner with minimal wait times, and the result is that the overall population remains both healthy and happy with the health care system of their country.

Most of us are also satisfied with the health care we receive here in Canada (Statistics Canada, 2008), perhaps in lieu of the health care reform debate raging in the United States. Yet, we have had the unpleasant experience of sitting in the waiting room of the doctor's office for countless number of hours, or perhaps know of someone who has had to wait months to receive treatment or diagnosis that should not have been delayed. The Canadian government is quite aware of this problem challenging both the health care providers and receivers alike, and is making an effort to find a solution. One such initiative is the investment of 4.5 billion dollars into the Wait Time Reduction Fund since 2004 (Health Canada, 2004).

With all of this in mind, I leapt at the opportunity to partake in a Public Health Exchange program through McGill's Global Health Programs to observe best practices adopted by Taiwan's health care systems, and how it came to serve its citizens so effectively and efficiently.

The expansion of health care in Taiwan mirrors its rapid economic development. After a strong economic growth of more than twenty years, the public of Taiwan demanded a better health insurance coverage in the 1980s, leading to a full-fledged national health insurance program. The new health insurance coverage arose from years of in-depth studies of health care systems from other nations. The health reform resulted in the NHI, which is now a government-run, single-payer system with universal coverage similar to that of Canada's. Prior to the establishment of NHI in 1995, 41 per cent of the Taiwanese population was uninsured – the majority of the uninsured were young children and seniors, whose need for health care is usually the highest. As a result of the mandatory enrollment the reform has since brought insurance to 99 per cent of citizens and legal residents, and increased the health care utilization rates of the uninsured up to par with those of previously insured populations (Cheng 2003).

Despite several similarities with the Canadian health care system as a whole, there are some notable differences between the two systems. Firstly, Taiwan's health care coverage is more comprehensive. It covers services that Canadians are usually pay out-of-pocket, or through supplemental health insurance. These services include prescription drugs, dental care, vision care and traditional Chinese medicine (Cheng 2003).

Secondly, patients are free to see doctors of any specialty without going through a referral or 'gatekeeper' system. There are also no limitations on the type of hospital that from which the patients can receive their health care. Due to the absence of a gatekeeper system, there is no need to first see your primary healthcare provider to receive a referral to see a specialist. As a result, there is virtually no waiting list for a visit to the doctor's office. There is also freedom to choose between health care facilities, ranging from small public health clinics to large private hospitals that offer comfort with luxurious décor.

Upon observing and learning about many health care facilities (including public and private clinics, large teaching hospitals, major public hospitals and private hospitals alike, to a psychiatric hospital, a Traditional Chinese Medical hospital and a regional Centre for Disease Control), and discussing with and listening to doctors, nurses, professors and medical students, the facilities appeared to be spectacular, well-equipped with modern technology; and the breadth of services available to the Taiwanese population presented was truly impressive.

With high health indicators comparable to any developed nation – infant mortality rate of 5.26 per 1000 births; and life expectancy at birth of 75.34 years for men and 81.2 years for women (Central Intelligence Agency, 2010) – it was clear that Taiwan was providing health care that successfully sustains a healthy general population. Furthermore, a closer look at Taiwan's national health expenditure rates indicate that this was being achieved at a fraction of the cost of other nations: only 6 percent of Taiwan's GDP is spent on healthcare, compared to 10 percent for Canada and 16 percent for the United States (Organization for Economic Cooperation and Development, 2010). Since its implementation, NHI has had a public satisfaction rating ranging from 70 to 80 per cent, dipping low only in the years where new policies introduced higher insurance rates (Cheng 2003). It remained unclear how Taiwan managed to sustain a health care system achieving similar, if not better, results than that of Canada's and the United States.

The NHI is publicly funded and financed on income-based premiums as opposed to general tax revenues. The premiums are based on payroll taxes paid by the employer, the employee and the government in varying amounts depending on different population groups. Most people who are employed pay 30 per cent of the premium, while their employer pays 60 per cent and the government subsidizes the remaining 10 per cent. The self-employed pay 100 per cent of the premium, and individuals from a low-income household are fully subsidized by the government. For the employed, the total insurance premium is typically 4.6 per cent of their

wages (Underwood, 2009), as well, the taxes from tobacco excise tax and the national lottery revenues are injected/infused into the system (Bureau of National Health Insurance, 2010).

The cost of the services from providers is covered mainly through reimbursements from the NHI, but it is also partially covered by co-payments from users (Cheng, 2003). The NHI is also supplemented by a co-insurance system where the user pays a nominal co-payment to the health care provider upon the use of its services. Its purpose is to discourage overuse. This may be compared to how wait times stemming from the referral-system in Canada discourages unnecessary hospital visits. The co-payment is usually a few dollars, or a fraction of the true cost of the service provided. The amount is capped by the NHI to eliminate any concerns of bankruptcy resulting from an accumulation of the fees. It is also waived for catastrophic diseases, individuals from low-income households or remote areas, infants and veterans.

One problematic area of health care that the NHI has tackled progressively is implementing the universal coverage and assuring similar health status between the indigenous and marginalized populations, and the rest of Taiwan. In order to eliminate disparities regarding access to health care, NHI has approached both the demand and supply side. On the demand side, it ensured that the population at risk were provided with insurance, and exempted them from co-payment. On the supply side, it has implemented an Integrated Delivery System (IDS), and guaranteed income for physicians practicing in remote areas (Bureau of National Health Insurance, 2010). Although certain disparities still exist policy tools such as IDS and rural payment bonuses contribute to continuous improvements (Chou, Huang et al., 2004).

Another innovation is the integration of traditional methods in a modern system. As traditional Chinese medical practice is an accepted form of medicine, and is a mainstream medical care in Taiwan. Chinese medicine is insured under the NHI. Traditional Chinese Medical (TCM) services ranges from acupuncture and fire cupping massages to medicinal herbs. It is believed to be effective in alleviation of many illnesses and disease, managing pain and promoting well-being. Traditional Chinese medicine is often used in conjunction with Western biomedicine (Chen, Chen et al. 2007) and accounts for six per cent of health expenditure on outpatient services in Taiwan (Bureau of National Health Insurance, 2010). However, not all TCM clinics are registered under the NHI, and standardization regarding the quality was not so straightforward.

As it turns out, the NHI began facing deficits in the late 1990s, relying on bank loans to pay health care providers. Between 1996 and 2009, NHI expenditures grew at an average of 5.27 per cent a year, exceeding NHI revenues with an average growth rate of 4.02 per cent a year (Bureau of National Health Insurance, 2010). The exceeding expenditures were a fault of the open-ended health insurance system relying on a Fee-For-Service (FFS) payment of the providers. The health care

providers performed unnecessary procedures and prescribed unnecessarily expensive drugs at the expense of the NHI. Submission of false reimbursement claims was another example of misuse of the system (Cheng 2003).

Due to the competitive nature of FFS, physicians were called upon to see an overwhelmingly large volume of patients per day, leading to rushed visits and insufficient time to get a complete patient history or conducting a thorough exam, which could lead to misdiagnosis, improper treatment or delays in proper treatment. This led to a vicious cycle of doctors ordering frequent follow-ups, which contributed to higher patient volumes and shorter visits. Moreover, many patients were led to believe/feel that their problems were not adequately addressed, resulting in repeat visits and 'doctor shopping' - visiting numerous practitioners simultaneously, and seeking unnecessary care, or care that does not require specialists, all further impinging on the system (Gunde, 2004).

To address some of these issues, the NHI made a number of changes in how the health care providers were reimbursed. From 1998 to 2002, a global budget policy was imposed on different sectors, replacing the Fee-for-Service system. The Global policy set an expenditure cap for each sector, whereby services provided beyond the cap would be reimbursed at lower rates. The new policy incentivized health care providers to stay within their set budget. Global budgeting proved to be effective, and overall growth rates of per capita medical spending declined in nearly all of the health sectors in the early 2000s. However, it was an incomplete solution as the NHI continued to face ever increasing expenditures.

In 2004, the NHI implemented a Resource-Based Relative-Value Scale (RBRVS) into the physician fee schedule, where physicians were paid according to the 'relative value' of services provided and the resources they consumed. It is based on the amount of physician-involving work that goes into the service, the practice expense associated with the service, and the professional liability expense for the provision of that service; also being adjusted according to the geographic region (American Association for Pediatrics, 2005).

The NHI continues to experiment with different methods of payment of provider. The most recent change to the health care system was in 2010, where the NHI introduced a diagnosis-related-group reimbursement (DRG) scheme to pay physicians. Under this scheme, the physicians are reimbursed at a certain rate for different types of patients according to their primary diagnosis (Bureau of National Health Insurance, 2009).

Further efforts to improve the quality of the NHI system led to the introduction of the IC (Integrated Circuit) Smart Card: a mandatory health card of sorts, but integrating innovative information technology. The Smart Card contains electronic data about the cardholder's personal identity, medical record, prescription history, remarks for catastrophic diseases, number of visits, administrative and expenditure information among other things (Smart Card Alliance, 2005). The introduction of

the Smart Card in 2002, had allowed Taiwanese hospitals and clinics to send electronic records on a daily basis to the Bureau of NHI, where the data is analyzed and audited on a regular basis. The Smart Card makes it possible to monitor high-utilization cases through patient profile analysis; prevent fraud from aberrant medical claims; and keeps surveillance of public hazards, tracking down suspects of communicable disease (Bureau of National Health Insurance, 2009).

The tracking of symptoms of communicable diseases is becoming increasingly important with the rise of pandemic disease, where persons infected must be identified and isolated as soon as possible to prevent the spreading of the infection. Although it is a relatively new system, preliminary results have indicated that the Smart Card has enormous potential to be a key tool in reducing infectious outbreaks, such as severe acute respiratory syndrome (SARS), through implementation of an on-line real-time mechanism for disease control, tracking and surveillance (Huang and Hou 2007).

Another major benefit from the use of Smart Card technology is the reduction in administrative costs due to improved administrative, billing and provider efficiencies. The technology has allowed for automatic operation of electronic transfer of medical records and bills, resulting in expedited reimbursements of providers. As the Smart Cards last for several years, it has also eliminated costs involved with frequent replacement of older health cards, which were previously made of non-durable material. As a result, Taiwan's health care system has the lowest administrative costs in the world, accounting for only two per cent of its total health expenditure. Comparatively, Canada spends 16 per cent of total health expenditures on administration and the United States spends 31 per cent (Woolhandier, 2003). The low administrative cost significantly contributes to how Taiwan has maintained the low rate of health expenditure spending over the accumulated GDP spending.

In spite of these efforts of new innovations and policy implementation, health care costs are still rising in Taiwan. The NHI's deficit is expected to reach \$3.2 billion US dollars by the end of 2010 if effective measures are not put into place. The government could increase spending from its GDP by raising the premiums although it would cause public unrest in the process. But even so, the extra income generated from increased premiums will only be a temporary measure in keeping the balance and offsetting the existing deficit of \$1.84 billion dollars US (Taiwan Today, 2010).

Taiwan is now looking overseas for other potential solutions. Medical tourism is a new and growing area in the world economy (Morgan, 2009) and it has come to the attention of the Taiwanese health care industry. In hopes of easing its growing deficit and financial burden, the Taiwanese government's Department of Health began planning distribution channels and marketing campaigns on medical tourism. Now, Taiwan brands itself as a home for first-rate medical care services (International Medical Tourism Journal, 2009). Taiwan has long been popular with its expatriate population as a medical-travel destination (Tung, 2010). However, the

market is expected to expand by several folds as Taiwan further opens its door to mainland China. With the recent lift of travel restrictions, 2009 alone brought 40,000 visitors from China to Taiwan to undergo health checkups and cosmetic surgery (Kastner, 2010).

Creating a system that is both financially sustainable and meets the needs of an evolving population is a fine balancing act with many factors. Taiwan will face health care challenges common to many other countries in the near future: an aging population; rising cost of the workforce in the medical health industry; and increasing costs of new technology and drug research and development.

The two weeks I spent in Taiwan taught me that there are no easy tricks to finding a solution to a problem. The development of the health care system is a continually evolving process that is sensitive to time, place, political and economic state of the country, and the needs of the people.

As it stands, the Taiwanese government is currently working on a 'second generation' NHI reformation, implementing new policies and strategies to make the health care system more sustainable (Bureau of National Health Insurance, 2010). Collaborating with other nations by sharing information on policy implications, research data, consultations and other innovations have led to the development and establishment of what is the NHI today. Further innovation and collaboration among nations can ensure that future steps taken to develop and to implement health care policies are more effective.

For now, Taiwan and the NHI stands as a successful case of how a nation was able to successfully established a universal health care coverage for the entire nation – almost from ground up. The system offers, at an affordable cost to the users, easy access to comprehensive health care of high quality. Despite some of the financial weaknesses it has shown and the downfalls it has faced in the last fifteen years, it is an example of how a government can strategically manage its resources in order to serve its people effectively; providing access to health care to those who need it most.

References

- American Academy of Pediatrics (2008). "Application of the Resource Based Relative Value Scale System to Pediatrics".
<http://aappolicy.aappublications.org/cgi/reprint/pediatrics;122/6/1393.pdf>
- Bureau of National Health Insurance (2010). "National Health Insurance in Taiwan".
http://www.nhi.gov.tw/webdata/AttachFiles/2010NHIprofile_990503.pdf
- Central Intelligence Agency. (2010, Nov). Taiwan. Retrieved November 2010, from The World Factbook: <https://www.cia.gov/library/publications/the-world-factbook/geos/tw.html>

- Chen, F.-P., T.-J. Chen, et al. (2007). "Use frequency of traditional Chinese medicine in Taiwan." *BMC Health Services Research* 7(1): 26.
- Cheng, Tsung-Mei (2003). Taiwan's new national health insurance programs: genesis and experience so far. *Health Affairs*, 22 (3), 61-76.
- Chou YI, Huang N, Chang HJ, Yip W. AcademyHealth Meeting (2004, San Diego, Calif). "National Health Insurance and Disparities in Access to Care in Rural Areas: A population-based study in Taiwan." *Abstr Academy Health Meet.* 2004; 21, abstract no. 1049. Retrieved November 2010 from <http://gateway.nlm.nih.gov/MeetingAbstracts/ma?f=103624083.html>
- Gunde, Richard. (Sept 30, 2004). "Healthcare in Taiwan: Opportunities and Success." *UCLA International Institute*. Retrieved 2010 from <http://www.international.ucla.edu/article.asp?parentid=15333>
- Health Canada. (2004, September 16). "First Ministers' Meeting on the Future of Health Care 2004: A 10-year plan to strengthen health care." Retrieved November 2010, from http://www.hc-sc.gc.ca/hcs/ssss/delivery-pretation/tpcollah/2004-fmst-rjms/index_e.html
- Health Canada (2008). "Healthy Canadians: Federal Report on Comparable Health Indicators 2008" <http://www.hc-sc.gc.ca/hcs/ssss/pubs/system-ragime/2008-fed-comp-indicat/index-eng.php>
- Huang E.W. and T.W. Hou (2007). "Design and prototype of a mechanism for active on-line emerging/notifiable infectious diseases control, tracking and surveillance, based on a national healthcare card system." *Computer methods and programs in biomedicine* 86(2): 161-170.
- IHS Global Insight (March 9, 2010). "NHI to See over US \$3 – bill Deficit in Taiwan, Health Minister Announces Resignation." Retrieved November 2010 from <http://www.ihsglobalinsight.com/SDA/SDADetail1E372.htm>
- International Medical Travel Journal (Dec 11, 2009). "TAIWAN: Taiwan government to promote inbound medical tourism". <http://www.imtj.com/news/7Entry1d62-172651>
- Kastner, Jens (October 5, 2010). "Taiwan's Medical Tourism Boom". *Asia Sentinel*http://www.asiasentinel.com/index.php?option=com_content&task=view&id=2736&Itemid=192
- Lu, H. J. P., & Hsiao, W. C. (2003). "Does universal health insurance make health care unaffordable? Lessons from Taiwan." *Health Affairs*, 22 (3), 77-86.
- Morgan, David. (October 2009). "Tracking the growth in Medical Tourism: OECD helps Ministers shape the debate." *Organization for Economic Cooperation and Development. Health choices*.
- Nelson, Chris (March 2007). "Taking the Cure: Medical Tourists." *Taiwan Panorama* P. 34 Retrieved November 2010 from http://www.sinc.gov.tw/en/show_issue.php?id=200739603034e.cat&cur_page=1&lsttype=table-2&n1=Finance%20and%20Economy&n2=&search=&height=&type=&scope=&border=&keyword=&lstPage=&num=8year=2007&month=03
- Organization for Economic Co-operation and Development. (2010) *OECD Health Data 2010*

- Held, T.R. (2008). Taiwan Takes Fast Track to Universal Health Care. NPR. <http://www.npr.org/templates/story/story.php?storyId=89651916>
- Smart Card Alliance. (2005). "The Taiwan Health Care Smart Card Project". http://www.smartcardalliance.org/resources/pdf/Taiwan_Health_Card_Profile.pdf
- Statistics Canada (2008) Healthy Canadians. A Federal Report on Comparable Health Indicators 2008
- Taiwan Today (March 9, 2010) Health minister resigns over health premium increase. <http://www.taiwantoday.tw/ct.asp?ntem=95660&ctnode=414>
- Tsang IK. Establishing the efficacy of traditional Chinese medicine. Nat Clin Pract Rheumatol 2007;3:60-1.
- Tung, Sarah (July 16, 2010). "Is Taiwan Asia's Next One-Stop Plastic Surgery Shop?". <http://www.time.com/time/world/article/0,8599,2004023,00.html#stz=06ep3Q9s>
- Underwood, Anne (Nov 3, 2009). "Health Care Abroad: Taiwan". The New York Times. <http://prescriptions.blogs.nytimes.com/2009/11/03/health-care-abroad-taiwan/?scp=6&sq=asia%20taiwan&st=cse>
- IHS Global Insight
- Zuelig Pharma (2006). "The expansion of medical tourism in Asia is proving a healthy boost for a growing number of the region's economies." The Market Partners. Issue 33, pg 8-9.

Zebra Technologies

**STATEMENT OF JIM L. KAPUT
SENIOR VICE PRESIDENT & GENERAL COUNSEL
ZEBRA TECHNOLOGIES CORPORATION**

**BEFORE A JOINT HEARING OF THE HOUSE COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEES ON SOCIAL SECURITY AND HEALTH**

“Removing Social Security Numbers from Medicare Cards”

Wednesday, August 1, 2012

Thank you, Chairmen Johnson and Herger and Ranking Members Becerra and Stark. I am Jim L. Kaput, Senior Vice President and General Counsel of Zebra Technologies Corporation, located in Lincolnshire, Illinois.

Zebra is a global leader in a variety of printing and marking technologies, including secure ID, RFID and real-time location solutions which all work to illuminate and secure mission-critical information to help customers take smarter and more secure business actions. Respected for our innovation and reliability, Zebra offers technologies that give a secure digital voice to assets, people and transactions, enabling organizations to unlock greater value.

I am pleased to submit this statement for today’s hearing record as Zebra is a strong supporter of H.R. 1509, the “Medicare Identity Theft Prevention Act of 2011”, which was introduced last year by Chairman Johnson and which currently has 48 bipartisan House co-sponsors. This bill, which would remove the Social Security number from the front of the Medicare card, would help reduce the danger of identity theft among America’s seniors, an issue that has been ignored for too long.

In addition to H.R. 1509, Zebra supports both H.R. 2925, the “Medicare Common Access Card of 2011” and H.R.3399, the “Medicare and Medicaid FAST Act. H.R. 2925 is sponsored by your colleagues, Congressmen Jim Gerlach (R-PA) and John Shimkus (R-IL), while H.R. 3399 is sponsored by another colleague, Congressman Peter Roskam (R-IL).

All three bills provide a solid foundation in the House for advancing the use of secure ID technology in the fight against identity theft and Medicare fraud. We are very appreciative of the efforts of all the authors and cosponsors of these three bills. We likewise applaud the pioneering efforts of your colleague in the other body, U.S. Senator Mark Kirk (R-IL), who is the author of S. 1551 and who previously represented Zebra Technologies during his tenure in the House.

Our company is prepared to offer our considerable technical expertise to the Subcommittees and to the House as you work to bring leading edge technology into the fight against identity theft and Medicare fraud through the passage of H.R. 1509 as well as the passage of H.R. 2925 and H.R. 3399. Our expertise in secure card technology is well recognized in both governmental and business circles and provides users with enhanced security, improved quality, lower costs and better customer service in applications that are analogous to and wholly supportive of the Subcommittees’ interest in advancing better protections against identity theft and Medicare fraud.

Thank you, again, for the opportunity to submit this statement in support of this legislation and the work you are doing on this very important issue.

